

# Cyber@UC Meeting 33

Katoolin, Special Project, and more...

# If You're New!


- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r** and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- Stay updated through our weekly emails and SLACK



# Announcements


- **National Initiative for Cyber Education Conference** was this week
- **CharitEweek** from Nov. 13th-Nov. 17th
- **Red team** against Franco's Class! *Nov. 30th - 1st Dec.*
- **P&G is prepping our visit.** After they complete the "*War-room*".
- **Logo Design** SUBMIT IDEAS!





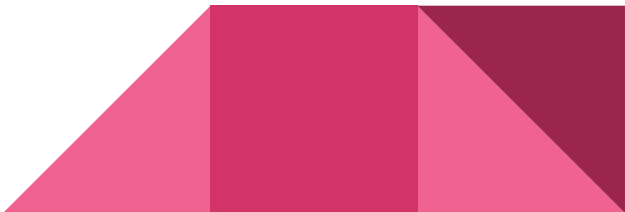
# National Initiative for Cyber Education (NICE) Conference summary

# Highlights

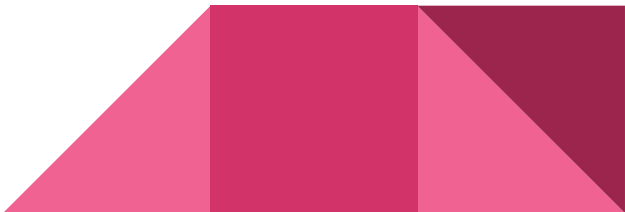
1. There are 300,000 cyber positions currently unfilled nationwide.
  2. UC is well positioned to lead the growth in Cyber
  3. There are multiple tracks for cyber careers
  4. Cyber@UC may be able to achieve national recognition through High School outreach efforts
  5. Cyber talent retention is a big problem
  6. There is a CAE NICE challenge to showcase cyber skills
  7. Skills required includes both technical and soft skills
- 

# Weekly Content

# Browser mining (update on malicious mining)

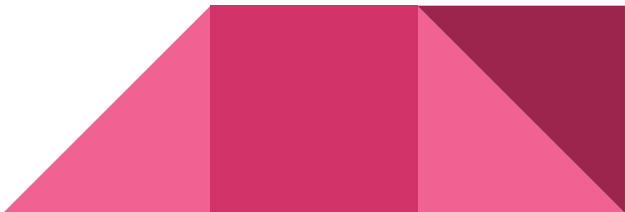
- Previously covered the installation of cryptocurrency miners being installed by attackers
  - Now, thanks to things like coinhive and jsminers, attackers are looking to infect websites by injecting code for these api into vulnerable websites
  - Typical targets are websites where users tend to visit for several hours at a time
  - Utilize the site visitors computing power
- 

# United front against cyber attackers

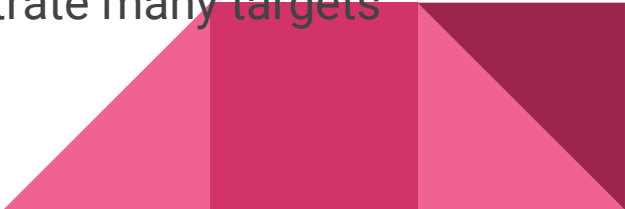
- Windows Defender has a program called Advanced Threat Protection (ATP)
  - Microsoft is now partnering with security companies BitDefender, Lookout, and Ziften
  - These are just the first companies Microsoft has partnered with, they have plans to add more companies to this list soon
  - These companies are allowing cross platform support for ATP
  - Each company will be feeding threat and alert information to each other through a Windows Defender ATP console
- 




# Keyloggers built-in to keyboards

- 104-key Mantistek GK2 Mechanical Gaming Keyboard was found to be silently recording key strokes and sending them to a server maintained by the Alibaba Group
  - Sent the key information through use of their cloud driver
  - Though it was found to record the number of keystrokes, users were not informed of the key logging
  - This could have been a lot more problematic if it had been a full key logger, especially since they were transmitting the information as plain text
- 

# New Cyberthreat group SowBug

- Now know they have been operating since at least 2015
  - Target South American and Southeast Asian government bodies and foreign policy institutions and steal sensitive data
    - Targeted countries include Argentina, Brazil, Ecuador, Peru, Malaysia
  - They like to use a (RAT) called Felismus to create backdoors into their target and can hide or extend its capabilities
  - Felismus was first identified late March, and enabled us to identify previous SowBug attacks
  - We know they are well funded because they can infiltrate many targets simultaneously
- 

# SowBug continued (How they work)

- It isn't currently clear how they infiltrate a network
  - They use malicious software updates of Windows and Adobe Reader to install their malware
  - They have also been known to use a tool called Starloader to deploy other malware and tools
  - Instead of compromising the software itself, they give it similar names to those used by the software and puts them in the directory where they can be mistaken for legitimate software
  - This hiding in plain sight approach has allowed them to remain hidden in systems for long periods of time
- 

# Source links

<https://www.darkreading.com/endpoint/cybercriminals-employ-driveby-cryptocurrency-mining-/d/d-id/1330353?>

<https://www.darkreading.com/endpoint-security/windows-defender-atp-extended-to-ios-macos-android-linux-/d/d-id/1330357?>

<https://www.microsoft.com/en-us/windowsforbusiness/windows-atp>

<https://thehackernews.com/2017/11/mantistek-keyboard-keylogger.html>

<https://thehackernews.com/2017/11/sowbug-hacking-group.html>

# Special Cyber Project

# Installing Katoolin

# Super Easy Commands!

1. `sudo apt-get install git`
2. `sudo git clone https://github.com/LionSec/katoolin.git && cp katoolin/katoolin.py /usr/bin/katoolin`
3. `chmod +x /usr/bin/katoolin`
4. `sudo katoolin`





*Breakout Session*  
Kali Linux Tools



# Choose a Tool and Research!

- Nmap
- THC Hydra
- AirmoN - ng, Airbase - ng, Aircrack - ng
- Hping3
- WafW00f
- Kismet
- Burpsuite
- Wireshark
- Recon - ng



Metasploit armitage

The hydra

WafW00f

Fierce

Hping3

Airmon - ng, Airbase - ng, Aircrack - ng

NMap

Recon - ng

whois Nslookup Dig

