Cyber@UC Meeting 46

Finishing up Direct Recon

If You’re New!

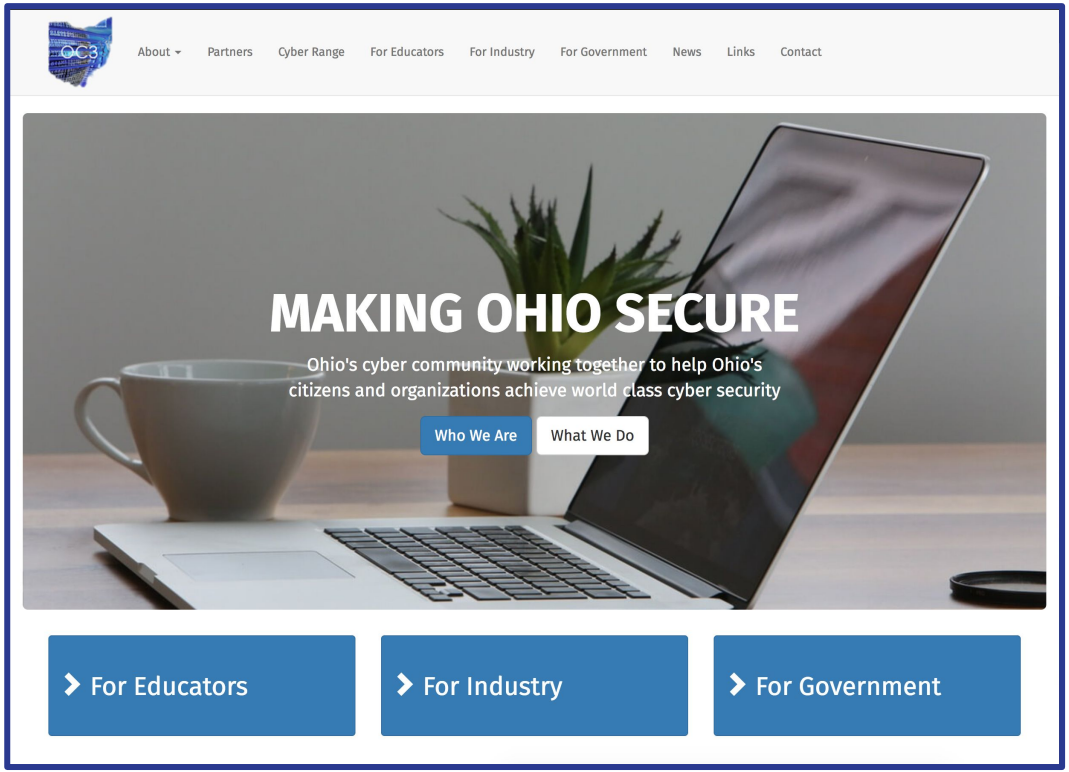
- Join our Slack **ucyber.slack.com**
- **SIGN IN!**
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- **Ongoing Projects:**
  - Malware Sandboxing Lab
  - Cyber Range
  - RAPIDS Cyber Op Center

Announcements

- **UC is slacking on equipment ordering**
- I hope everyone had a **great Spring Break**
- **Lakota East Outreach** to happen again soon
- Cincinnati B-Sides on **May 12th**, registration not open yet

OC3 website

- WordPress → Drupal
- Vicki presented it in Columbus on Tuesday



Public Affairs

- Please fill out Google form for **GroupMe** Numbers!
  https://goo.gl/forms/94i9kMJgtpDGXsC22
- Our brand new **YouTube** channel has just been made. We will be live streaming meetings, events, etc and posting relevant videos to the channel. Please subscribe!
  youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us on our social media:

Facebook: facebook.com/CyberAtUC/

Twitter: twitter.com/UCyb3r

Instagram: instagram.com/cyberatuc/

Website: ucyber.github.io

Weekly Content

MOSQUITO Attack: data flow over air-gap

- Using ultrasonic waves, two or more computers can covertly share data
- Air-gapped computers are commonly used to maintain security for a company’s network
- This attack works by reversing connected speakers, headphones, and earphones to work like microphones
- Requires both computers to be infected in some way by an attacker
  - Perhaps through removable media
- Maximum distance listed is 9 meters, about 30 feet

MOSQUITO sources

https://thehackernews.com/2018/03/air-gap-computer-hacking.html

https://thehackernews.com/2018/02/airgap-computer-hacking.html

https://arxiv.org/pdf/1803.03422.pdf

The end of the first article contains links to a bunch of other hardware covert data transfer exploits these guys have found in the past

Trojanized BitTorrent Software mines crypto

- A popular BitTorrent client called MediaGet was compromised a little over a week ago
- A malware called “Dofoil”, or “Smoke Loader”, was being placed on windows machines and mining Electroneum using the victim’s CPU
- Dofoil managed to infect computers in Russia, Turkey, and Ukraine on March 6th
- Microsoft’s Windows Defender research department found and blocked the attack before it could cause serious damage
- MediaGet appears to be a victim of supply chain attack
    - Similar to CCleaner hack from last September

MediaGet (continued)

- Almost 400,000 devices were infected
- Windows Defender was able to detect and block the malware
- Microsoft states that AI-based machine learning techniques and behavior monitoring used by Windows Defender played a key role
- A legitimate, signed version of mediaget.exe downloads update.exe
- The poisoned update.exe downloads and installs an infected mediaget.exe that is unsigned
- The poisoned update.exe is signed by a third party and signed with a different cert to get through the signing requirements of mediaget.exe

MediaGet (sources)

https://thehackernews.com/2018/03/windows-malware-hacking.html

https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/poisoned-peer-to-peer-app-kicked-off-dofoil-coin-miner-outbreak/