

# Cyber@UC Meeting 75

MITRE Framework Continued

# If You're New!

- Join our Slack: [cyberatuc.slack.com](https://cyberatuc.slack.com)
- Check out our website: [cyberatuc.org](https://cyberatuc.org)
- **SIGN IN!** (*Slackbot will post the link in #general every Wed@6:30*)
- Feel free to get involved with one of our committees:  
*Content Finance Public Affairs Outreach Recruitment*
- Ongoing work in our research lab!



# Announcements

- Emblem Updates!
- NSA internships
  - Application window closing **TOMORROW**
- US Bank Partnership in the Works!
- Chipotle fundraiser
  - Saturday Nov 3rd, 4pm–8pm
- Officer elections Today end of meeting



# Election nominees *(incumbents shown in parentheses)*

## **President** *(A.J. Cardarelli)*

A.J. Cardarelli

Clif Wolfe

Ryan Young

## **Vice President** *(Hayden Schiff)*

Hayden Schiff

## **Treasurer** *(Ryan Baas)*

Ryan Baas

Clif Wolfe

## **Secretary** *(Mike Sengelmann)*

Timothy Robert Holstein

## **Head of Content** *(Cory McPhillips)*

Christopher Morrison

## **Head of Finance** *(Kyle Hardison)*

Kyle Hardison

Ryan O'Connor

## **Head of Public Affairs** *(Jai Singh)*

John Igyarto

Jai Singh

## **Head of Outreach** *(Mahathi Venkatesh)*

Mahathi Venkatesh

Ryan Young

## **Head of Recruitment** *(Greg Barker)*

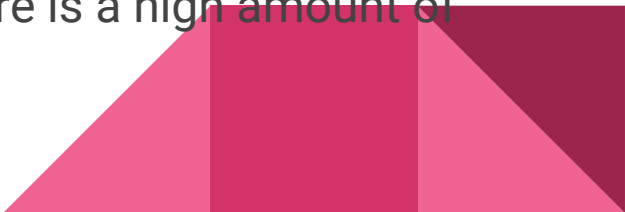
Greg Barker

# Weekly Content

# Windows Zero-Day

- PoC posted to GitHub
- Privilege escalation flaw in the Microsoft Data Sharing dssvc.dll
- Local service running as LocalSystem account
  - This has lots of privileges because it provides data brokering between applications
- Allows the deleting of critical system files
- Ex. Delete important dll, hope victim looks for it in more writeable location
- Only on Windows 10 and recent versions of Windows server
- Second time this researcher released a Windows zero-day in < 2 months
- Days after his previous disclosure, the exploit was found in the wild
- Once again, he has chosen not to wait the standard 90 days
- Beware until next month's patch tuesday, Nov 13

# DustSquad

- Russian APT
  - Primarily target Central Asian users and diplomatic entities
  - Use Delphi as language of choice, apparently this is unusual
  - Make great use of Octopus3.php malware, back in 2017
  - New version of Octopus found in April 2018, pretending to be Telegram Messenger w/ Russian interface
    - Malware seems to be simple
  - Most likely relying on Telegram ban in Kazakhstan
  - Between DustSquad and other APTs, we can see there is a high amount of interest in the Central Asia region
- 

# Recommended Reading

<https://thehackernews.com/2018/10/android-security-updates.html>

<https://krebsonsecurity.com/2018/10/mirai-co-author-gets-6-months-confinement-8-6m-in-fines-for-rutgers-attacks/>

<https://krebsonsecurity.com/2018/10/how-do-you-fight-a-12b-fraud-problem-one-scammer-at-a-time/>

<https://thehackernews.com/2018/10/ibm-redhat-tech-acquisition.html>





# Recommended Reading (continued)

<https://thehackernews.com/2018/10/facebook-cambridge-analytica.html>

<https://thehackernews.com/2018/10/russia-triton-ics-malware.html>

<https://thehackernews.com/2018/10/privilege-escalation-linux.html>

<https://thehackernews.com/2018/10/windows-defender-antivirus-sandbox.html>



MITRE ATT&CK

*Initial Access*

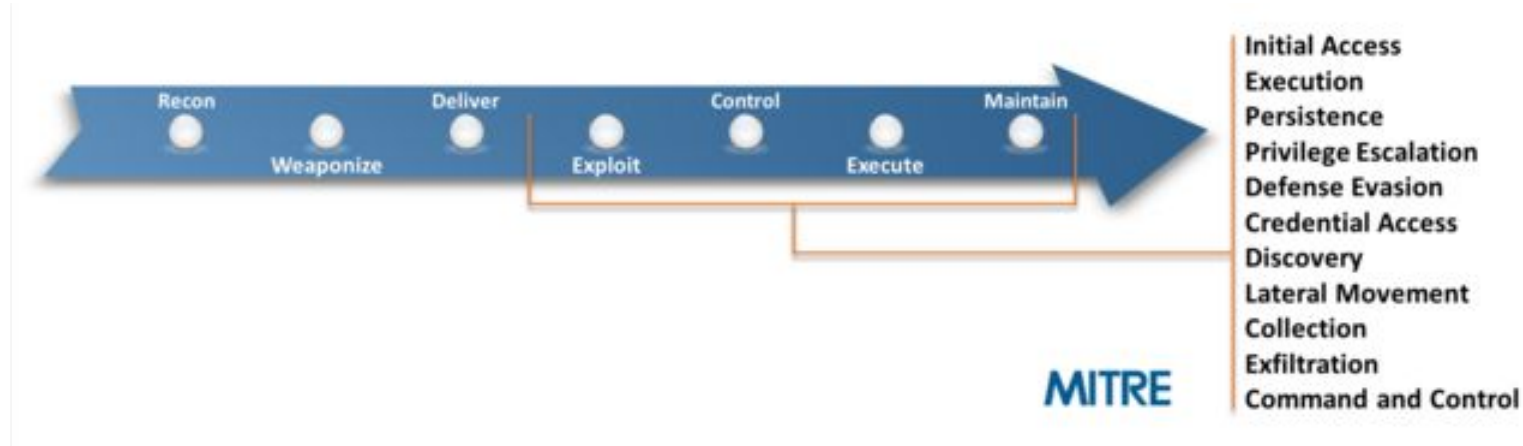
christopher@CRONUS:~\$ █

# The Topics Today Go Something Exactly Like This

- ATT&CK Techniques and the Cyber Kill Chain
- Initial Access Techniques
- Some Examples
- Backdoor Factory Exploration



# ATT&CK and the Cyber Kill Chain



# Initial Access Techniques

Computer Vectors	Human Vectors
Drive-by Compromise	Malicious USB's
Exploit Public-Facing Services	Spear Phishing Attachments/Links
Supply Chain Compromise	Spear Phishing Via Services
Valid Accounts	Trusted Relationships \ Spys



# Technique Implementations

USB Rubber Ducky - Emulates a keyboard to abuse trusting USB devices

Bash Bunny - Same thing but has networking capabilities

Poison Tap - Project from SAMYK that routes all of the internet traffic through itself over USB as a MiTM and back door installer.

**ALL of these are commercially available / open source and some have even more undetectable sneaky in the security research field.**



# Workshop: Backdoor Factory

Backdoor factory is a research utility for injecting backdoors into DLLs/EXE's

No longer developed, and only for research purposes

Included in Kali, otherwise clone the git repo

Inject a backdoor into an executable then upload it to VirusTotal to see which anti-virus systems would detect it.

**`./backdoor.py -h`**

**<https://github.com/secretsquirrel/the-backdoor-factory>**



# Elections



[bit.ly/cyberatucvote](https://bit.ly/cyberatucvote)

