

# UC.yber; Meeting 25

Vulnerabilities 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

- **Day-con cybersecurity conference** in Dayton Ohio Sept. 21, 22, 23
  - Packetwars!
- **October 27/28th ACM** programming challenge
- **P&G cybersecurity center** tour is still in the planning phase
- **National Collegiate Cyber Defense Competition** prepping will begin soon
- **Cyber range meeting** on use cases



The background is a solid pink color. In the top right corner, there are several overlapping geometric shapes: a dark pink square, a medium pink square, and a light pink square, all partially cut off by the edge of the frame.


# Weekly Info Session

# Xafecopy Trojan

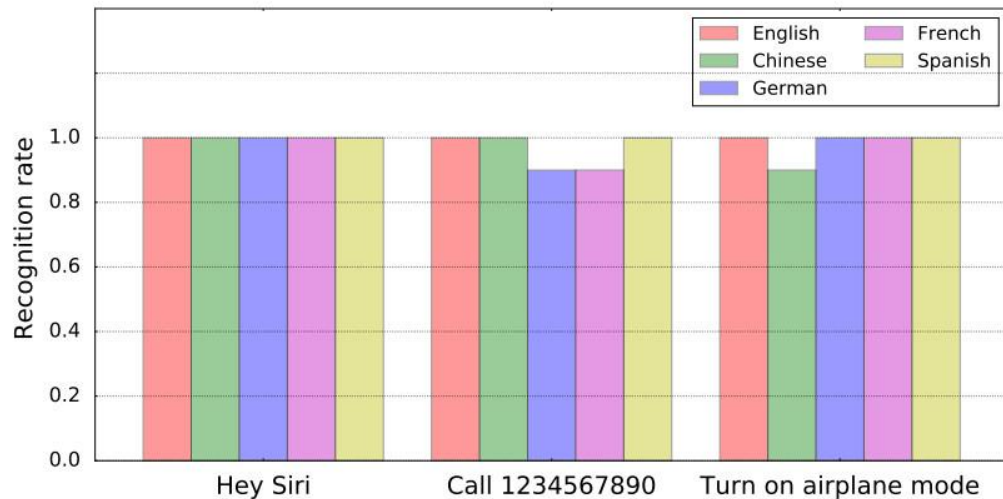
- Targets Android phones.
- 4,800 users , 47 countries in a month.
- Masks as a useful app (Usually as a Battery optimizer).
- Opens url's with WAP billing.
- Charges directly to the user's mobile carrier bill.



# The Dolphin Attack

- Is your voice assistant taking orders behind your back?
  - Scientists from China's Zhejiang University found a way to do it.
  - Created a program to convert normal voice commands to frequencies higher than 20Khz.
  - They named this Dolphin attack because dolphins and bats use high frequency noises for echolocation.
  - This attack can be used to download a malware from a website or initiate a phone call.
- 

Dolphin attack can be used to give commands in different languages.



The attack needs to take place in a fairly quiet environment.

A Dolphin attack that asks siri to turn on airplane mode was 100% successful in an office, 80% in a cafe and 30% when on a street.

Since voice assistants respond audibly to commands, the chances of hacking your phone without your notice are slim.


One way to fix this would be for the phone to ignore any commands outside a certain frequency range.

<https://www.youtube.com/watch?v=21HjF4A3WE4>





# Threat Deception:Defending against cyber attacks

- On average, security compromises take 100 days to be found, and usually by some external source
  - Predict 10% enterprises will be utilizing threat deception by 2018
  - Operates from the ideology that an intrusion will occur eventually
  - Attempts to deceive attackers and lead them to false data
  - Allows the defenders to gather valuable info on the attackers
  - Reduced false positive reports for the defenders
  - <https://www.darkreading.com/threat-intelligence/deception-a-convincing-new-approach-to-cyber-defense/a/d-id/1329839?>
- 



# Web Vulnerabilities with bWAPP

# OWASP Top 10

1. Injection
2. Broken authentication
3. Cross site scripting (XSS)
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function level access control
8. Cross-site request forgery (CSRF)
9. Using component with known vulnerabilities
10. Unvalidated redirects and forwards



# Bee-Box Virtualbox Setup

1. Install Virtualbox (<https://www.virtualbox.org/wiki/Downloads>)
2. Install Bee-Box (<https://sourceforge.net/projects/bwapp/files/bee-box/>)
  - 1.2 Gb File
  - Install unzipping software for 7zip files (Keka for MacOS)
3. Open Virtualbox and select “New”
4. Name = Bee-Box      Type = Linux      Version = Ubuntu (64-bit)
5. Allocate at least 1.2 Gb of RAM
6. Use existing virtual hard disk file
  - Select bee-box.vmdk from unzipped Bee-box folder



# OS Command Injection

# What we will leverage

nc = netcat used to read and write data over a network

-v = verbose output

-l = listen for an incoming connection rather than initiate a connection to a remote host.

-p = port for communication

;; = end of command character

<https://github.com/theand-fork/bwapp-code/blob/master/bWApp/bwapp-command-nc.py>

# Shellshock Vulnerability