cyber@ucr:~$

Welcome Hackers!

Day 04/10/2019

Check In: https://r.ucrcyber.org/checkin

What is Cyber@UCR?

- Learn the ins and outs of cyber security
- Participate in cyber security related competitions
- Find careers in cyber security in companies such as:
  - Raytheon
  - Qualcomm
  - SoCal Edison
  - FBI

Security in the news:

- Daniel with Cloudflare news

Spring Plan:

- 5 General Meetings (DAY TIME LOC):
  - Bug Bounty
  - HID attacks
  - Exploiting / Hardening the Linux Kernel
  - OTA (Bluetooth / WiFi / radio)
  - Windows Active Directory Hacking
  - Red Team architecture and tools
- Red Team / CTF Meetups
  - Spyware
  - Ransomware
  - Code Analysis
- Blue Team / CCDC Meetups
  - Forensics
  - Log Analysis
  - Tabletop
  - Network Segmentation

CCDC

- Defense oriented team competition
- Defend against professionals in the field as you perform the role of a system administrator in a business-like setting
- Interested?
  - Join ucrcyber.slack.com and tell us you wanna compete!

Upcoming Events:

1. CCDC TBD
2. CTF TBD

Join Us

- Mailing list:
  - r.ucrcyber.org/email
- Slack:
  - Ucrcyber.slack.com
- Facebook:
  - facebook.com/groups/ucrcyber

HID attacks

Everyone must sign an ethics form before we begin!

What is a HID and why is it yelling?

- HID stands for Human Interface Device.
- Examples: keyboards, mice, USB ethernet/Bluetooth adapter, etc . . .

How can this be exploited?

- By preprogramming keystrokes onto a device that emulates a keyboard, we can inject them into the computer so we can type at inhuman speed!
- We can make the computer open a terminal, git clone an evil repo, and launch a custom nc process in the background and now we have a backdoor in about 30 seconds!
- This is also used for exfiltration! Save password files to its storage.

Why does this work?

This abuses the computer's inherent trust of USB devices not validate whether or not a human is using them. This vulnerability is most commonly called the BadUSB or the USBDriveBy.

Variants!

1. USB Rubber Ducky, made by Hak5
2. USBDriveBy, Malduinos predecessor made by Samy Kamkar
3. Malduino, device is made by Seytonic, idea has been around
4. PoisonTap, uses a RaspberryPi Zero and works on locked machines
5. OMG-cable, send payloads OTA via charging cables for iPhones and Androids.

There are a lot more but there are more or less a variant on these, ie Bash Bunny, LAN turtle, etc

USBRubberDucky

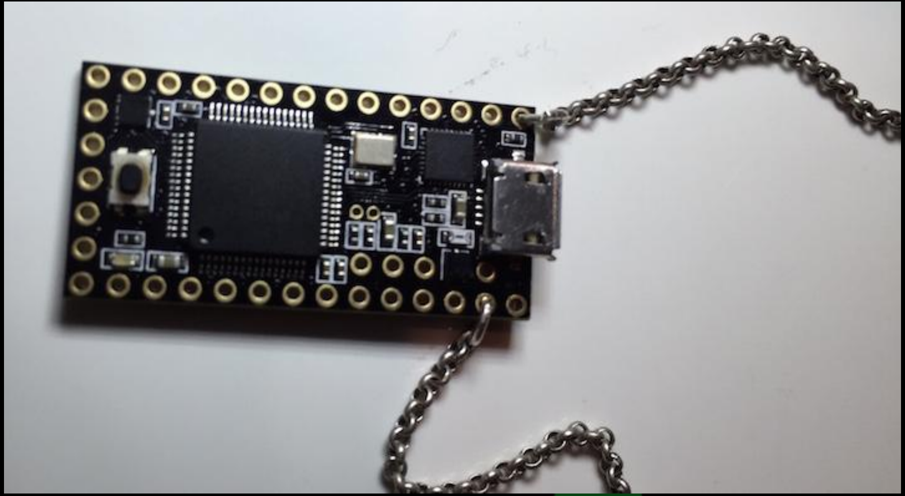
USB Rubber Ducky: Developed and sold by Hak5, this device tells the computer that it is a keyboard which allows it to inject malicious keystrokes.

With a MicroSD card slot, you can put a large payload on it and with a simple case, it looks like any other generic USB. No one suspects any difference :)

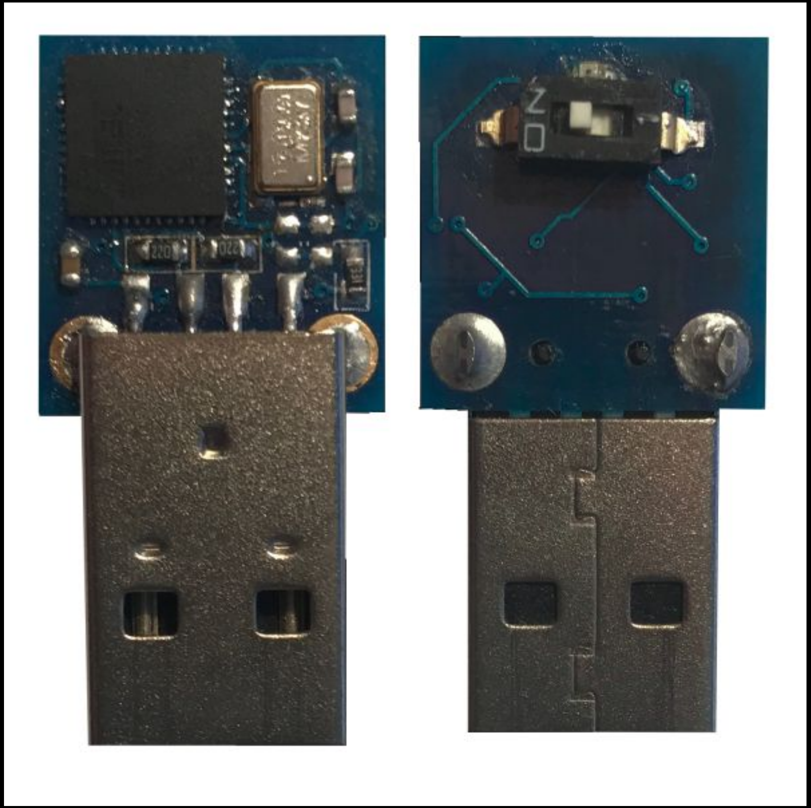
Uses “DuckyScript” to write out payloads.

USB DriveBy

Uses a Teensy microcontroller to emulate a Keyboard and mouse to inject malicious keystrokes AND click dialog boxes (like “Run as Admin”). This version spoofs the victims DNS to send them to malicious websites that are not real.



Malduino (Arduino Variants)



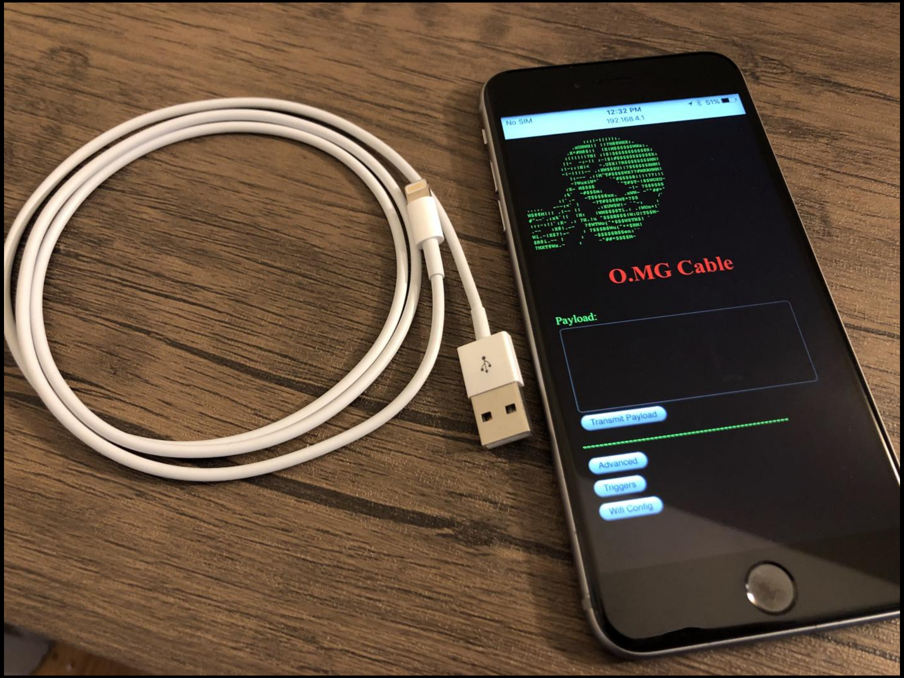
Very similar to the Teensy implementation as both use a microcontroller as opposed to a usb. Uses C/C++ to do what the Ducky can do.

PoisonTap

Hijacks the internet traffic (whether the machine is locked or not) and can access the LAN. I'm tired of typing so here is Samy Kamkar’s summary

When PoisonTap (Raspberry Pi Zero & Node.js) is plugged into a locked/password protected computer (Windows, OS X or Linux), it: - emulates an Ethernet device over USB (or Thunderbolt) - takes over all Internet traffic from the machine (despite being a low priority network interface) - siphons and stores HTTP cookies from the web browser for the Alexa top 1,000,000 websites - exposes the internal router to the attacker, making it accessible remotely - installs a persistent web-based backdoor in HTTP cache for hundreds of thousands of domains and common Javascript CDN URLs, all with access to the user’s cookies - allows attacker to remotely force the user to make HTTP requests and proxy back responses (GET & POSTs) with the user’s cookies on any backdoored domain - does not require the machine to be unlocked - backdoors and remote access persist even after device removal

OMG cable



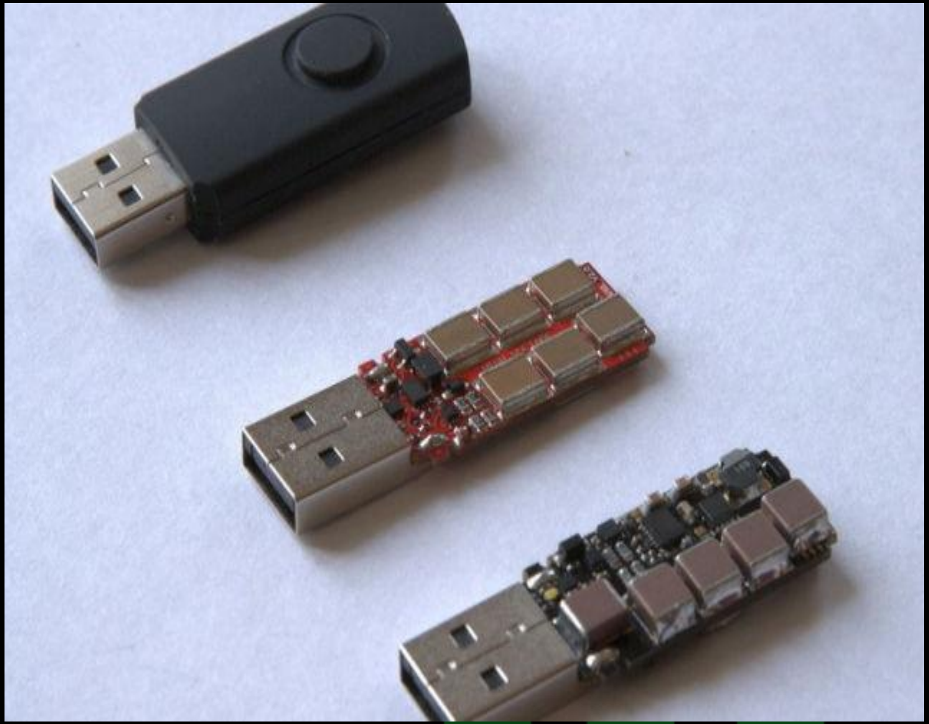
@_MG_ developed this after about ~$4000 and ~300 hrs of working in his spare time. Its a regular USB charging cable but with a twist! It has a malicious USB embedded into it that you can connect to from your phone and inject payloads!

You know it's for real 1337 H4x0r$ when there is a skull done in ASCII art in green on black. For the ult edge!

What if I don’t want to steal anything?

Then you must be looking for the USBKiller!

Its a USB with some capacitors that it charges up when it's plugged in and once full, it releases it back on the same powerline, frying the motherboard or USB connection.



DEMO TIME!

Everyone must sign an ethics form before we begin!

Process

1. Get physical access to the device.
2. Plug in the USB, or arduino.
3. Wait for it . . .
4. Profit.

In real practice it's actually a little harder

The reason for this is because there are so many different machines that run at different speeds so if you put a delay of 300ms in between each keystroke but you're attacking an older computer, it might miss the keystrokes and malfunction or not deliver the payload. Ideally you want the delays to be long enough to where it works on most machines but not too long so you're standing there for half an hour.

Time to see it in action!

Does anyone have a MacOSX or Windoz machine?