Building Trojan Hardware at Home

JP Dunning “.ronin”
BlackHat Asia 2014

What is Hardware?

- PCB (Printed Circuit Board)
- Single use components (resistor, led, crystal, capacitor, etc)
- Specialized chips (RAM, controller, I/O)
- Primary processor chip
- I/O ports
- Firmware

Goals of This Talk

- Discuss hardware and firmware based Trojans
- Remain platform neutral
  - This is not a vendor specific problem
- Display the relative ease of modifying hardware

What you'll need to play along

- Computer with Linux and Windows
- Cheep used target hardware
- Less that $40 programmer
- Time
- Soldering equipment (sometimes)
- Trojan
- (Minions)

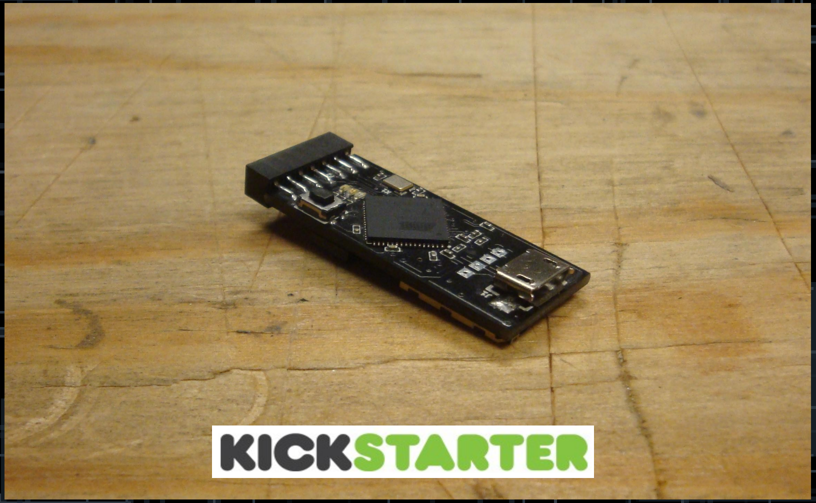
Modify Hardware

- What's in the Box?!?!
- What kind of IO ports are available?
  - USB, UART, I2C, SPI, PS/2, RJ45, GPIO, draughtboards connectors, etc.
- Get it cheep
  - Ebay/Craigslist/Taobao anyone?!?
- What is the hardware's purpose
- How does is interact with target

USB + 1

- Let's hide out attack hardware inside a USB device
  - Many devices have large open cavities
  - Looks the same from the outside
- Attack the host device connected to the USB Trojan
- Try to leave device functional

The Glitch Platform



- Create an open hardware testing platform
- Make it Arduino compatible
- Build upon open hardware security projects
- Make projects accessible to non-coders and non-engineers

Glitch Platform made Easy

- Create or edit modules on the Micro SD card using plaint text configuration files
    - Available configuration options are up to the developer
    - Provide additional payload files
- Select module with DIP switch
- Plug-and-play
- Project site
    - theglitch.sourceforge.net

Keystroke Injection

- Emulating computer keyboard
  - “Press” keys
- Benefits of leveraging HID Injection
  - “Type” accurately
  - “Type” quickly
  - No Human Required
- Works against computers that can use an external keyboard
- Designed for Windows, Linux, and OS X

HIDIScript

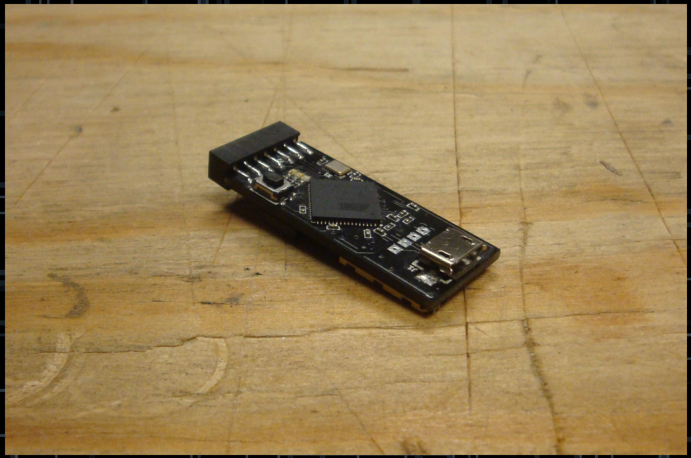
- HID Scripting Language
- Four components
  - Plain text
  - Parsed Modifiers
  - Parsed Keys
  - Commands
- Write using HIDIScript Generator
  - http://keymeglitch.sourceforge.net

HIDIScript Example

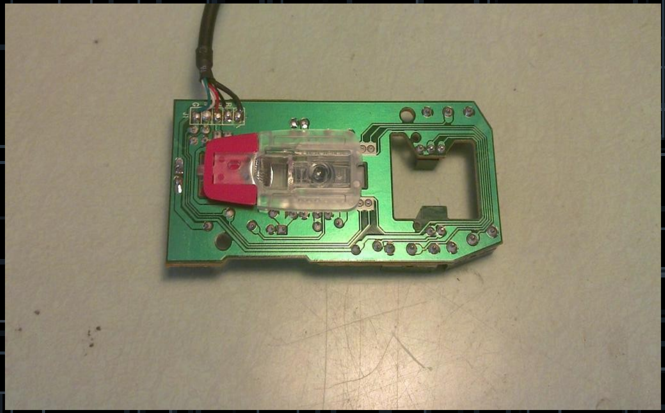
```
[KEY_RIGHT_GUI][KEY_R]

[WAIT_1000]

notepad

[KEY_ENTER]

[WAIT_2000]

Hello BlackHat Asia 2014!

[WAIT_2000]

[KEY_ALT][KEY_F4]
```

Trojan Mouse

- Parts
  - USB mouse
  - USB hub
  - The Glitch

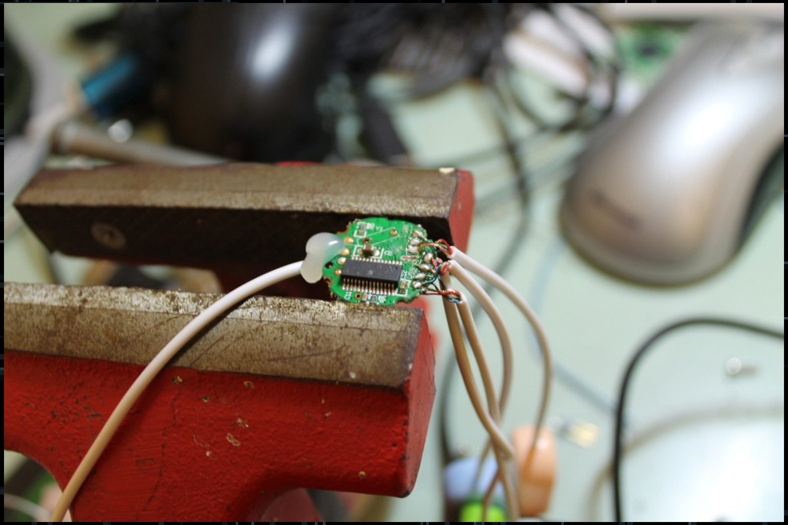


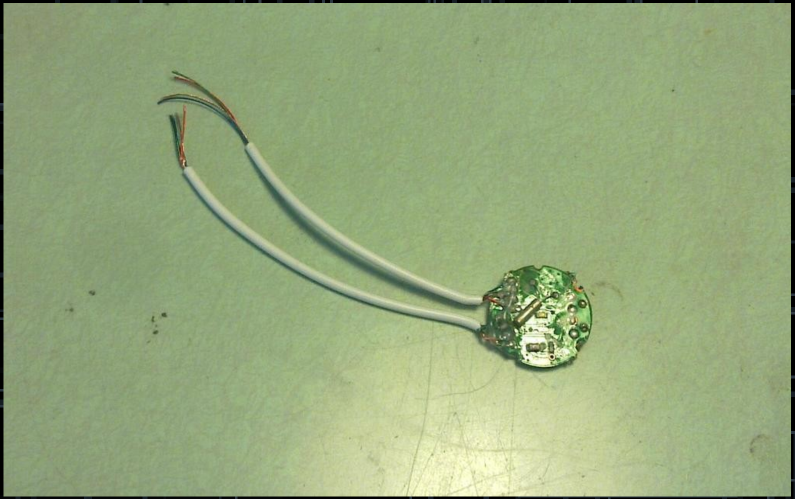
Trojan Mouse



- Open the mouse
  - USB Pins solderer or plug in
  - Remove scroller
  - Several square centimeters of open space

Trojan Mouse





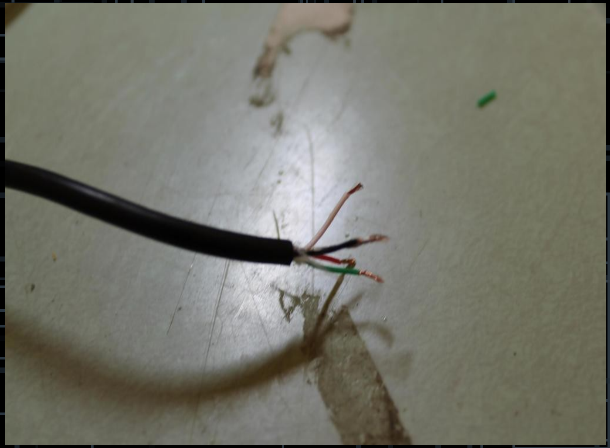
- Remove the hubs case
- Cut of USB plugs
- Unsolder two cables
- Unsolder USB host connector

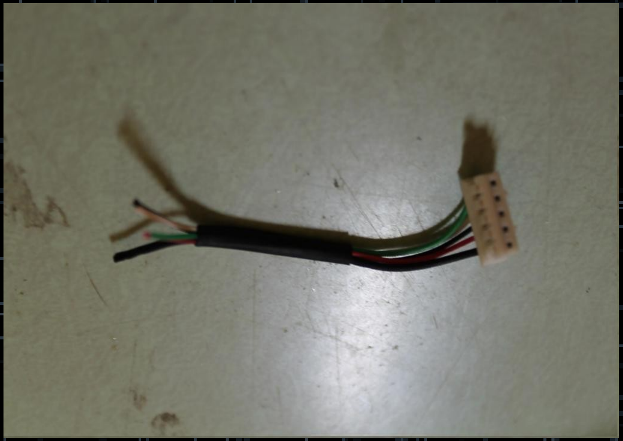
Trojan Mouse

- USB (Universal Serial Bus)
  - Four pins
    - Vcc <---> Vcc (Red)
    - D- <---> D- (White)
    - D+ <---> D+ (Green)
    - GND <---> GND (Black)
  - Standard colors
    - Many USB cables use the standard color wires
    - Makes it easy to reuse cables

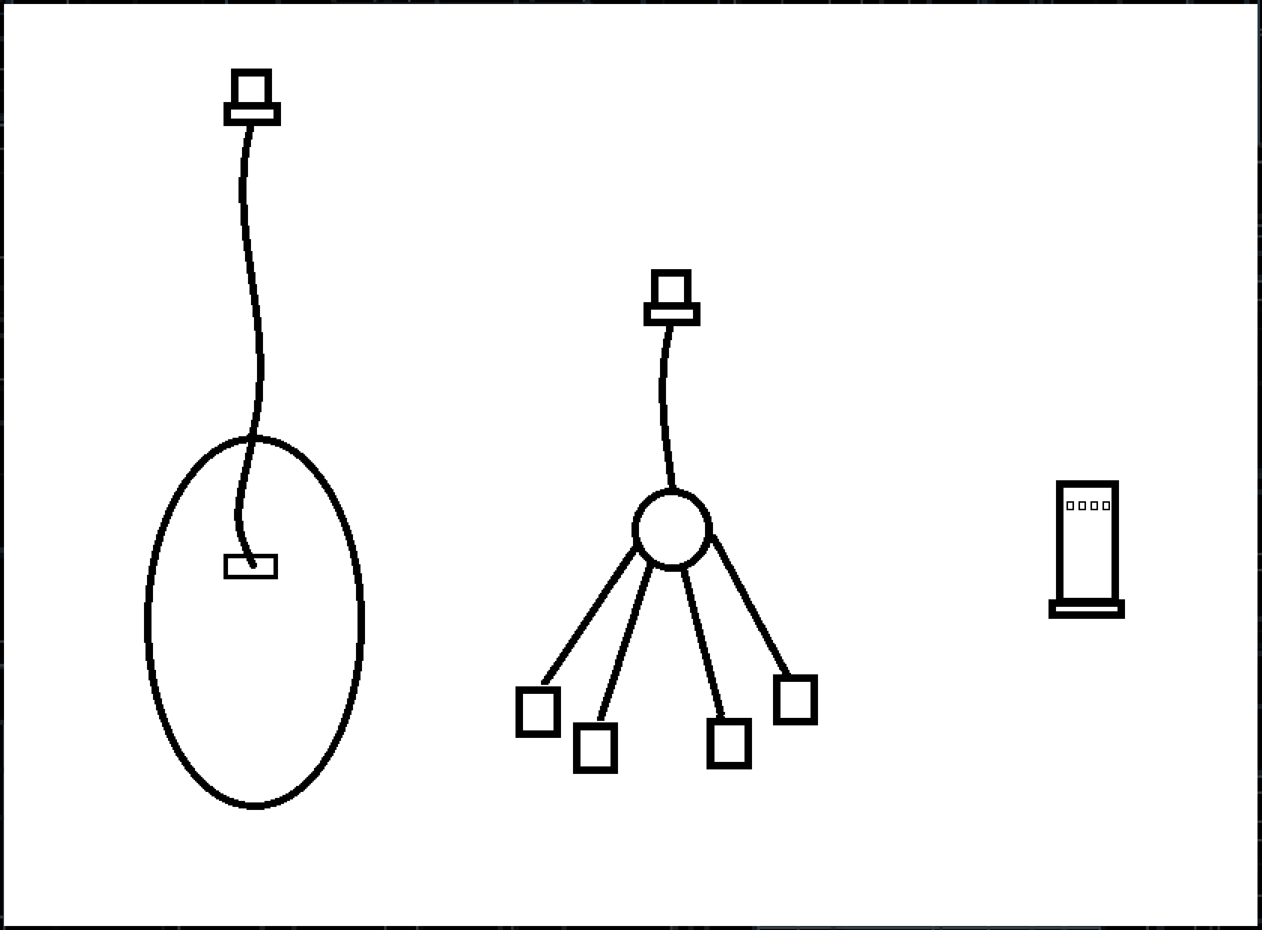
Trojan Mouse

- Split the mouse USB cable

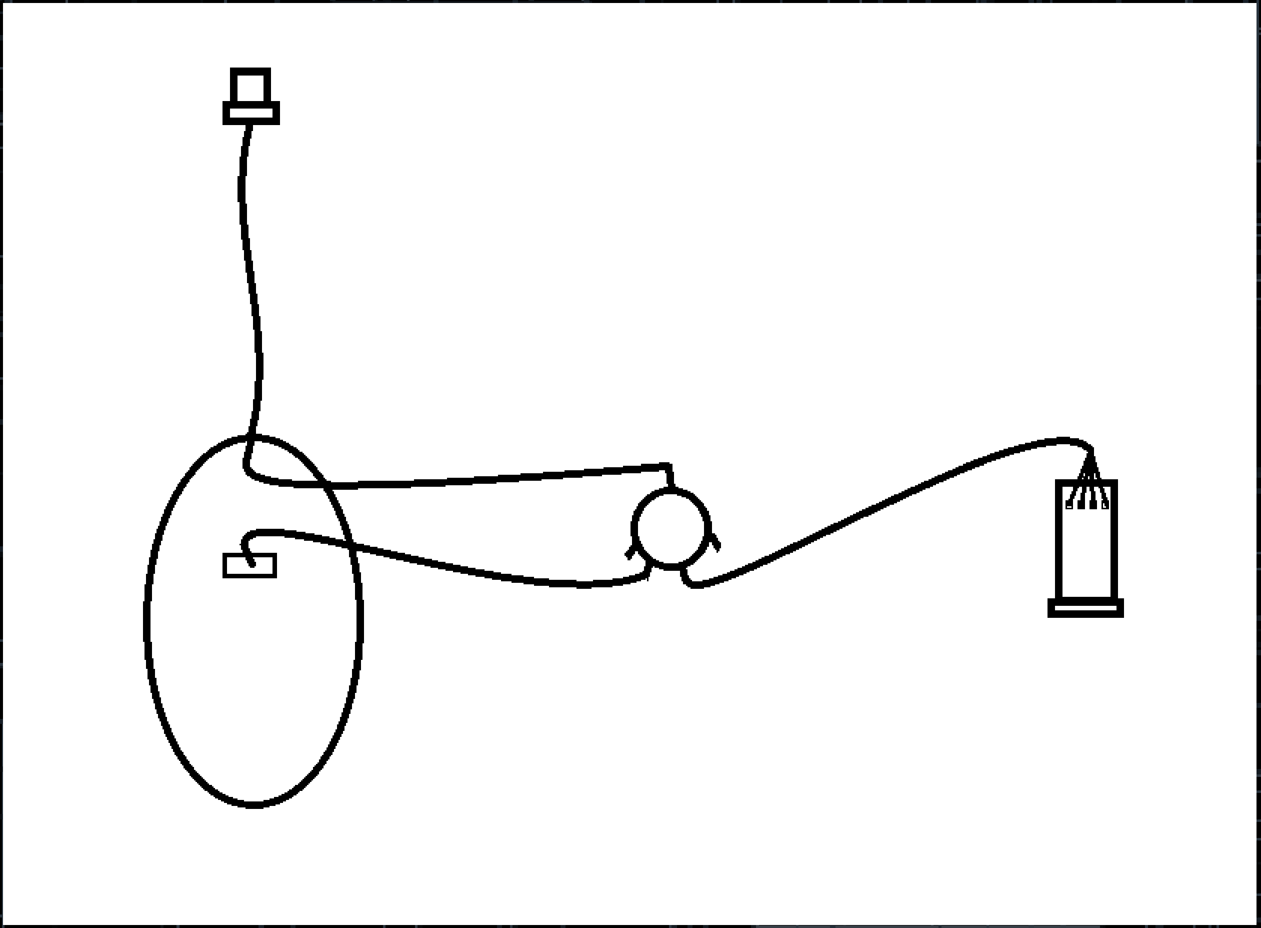




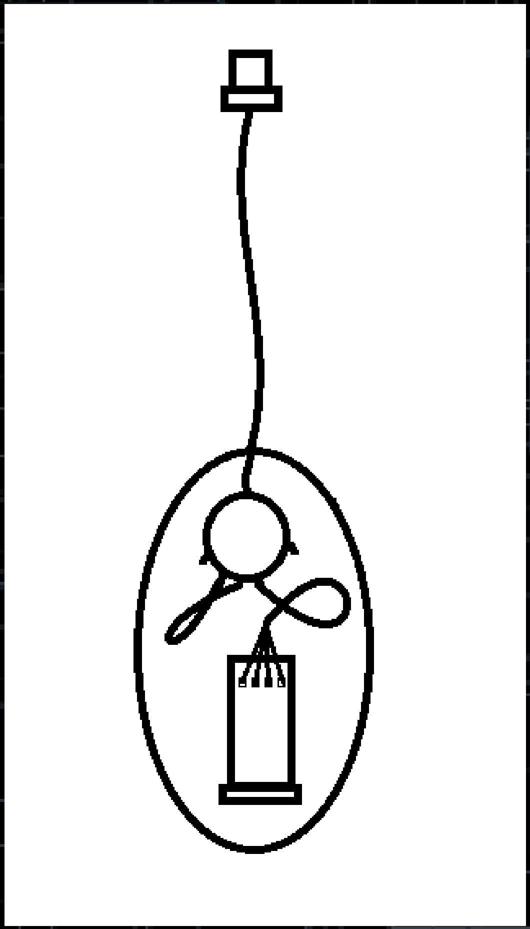
Trojan Mouse



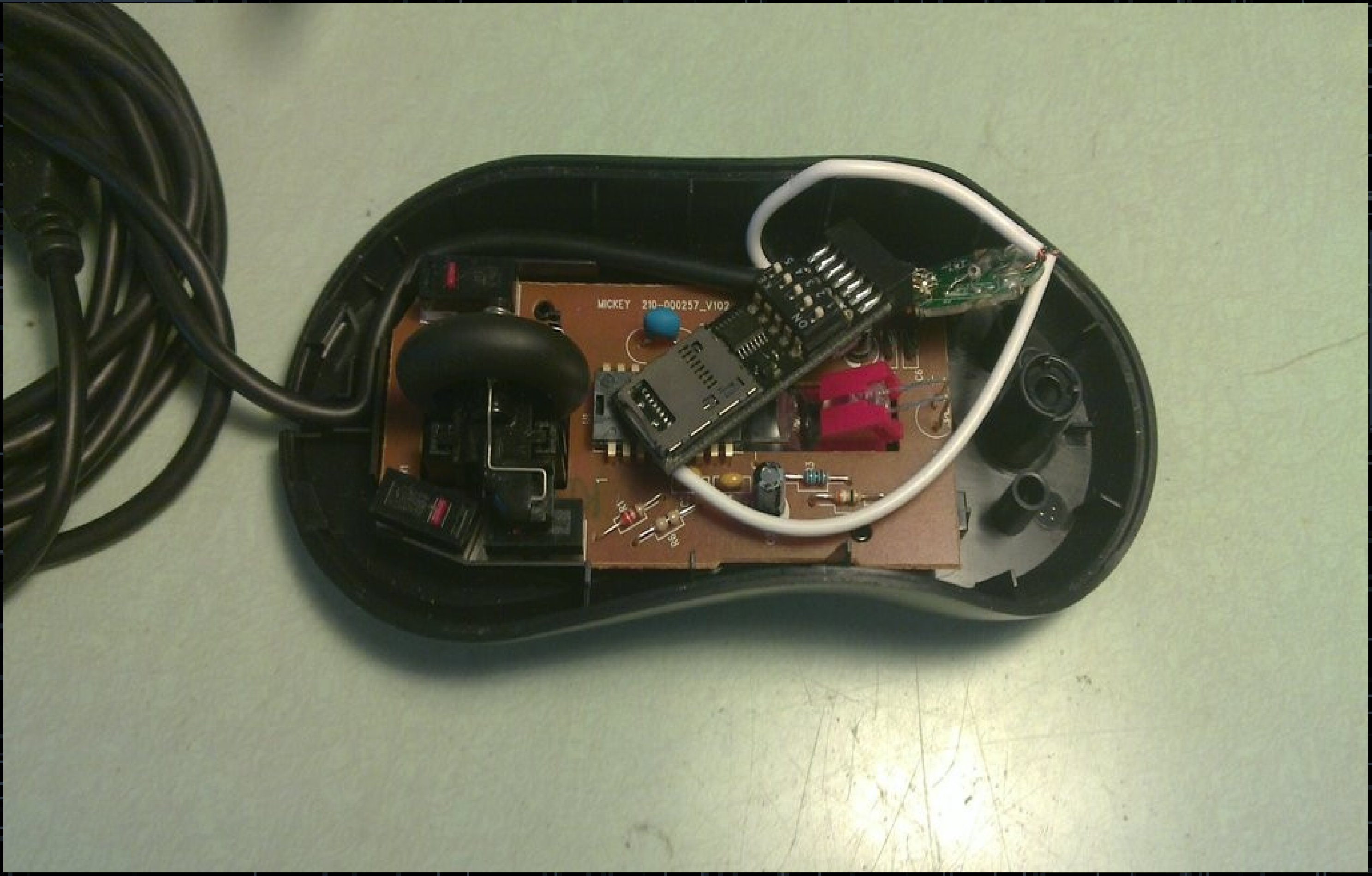
Trojan Mouse



Trojan Mouse



Trojan Mouse



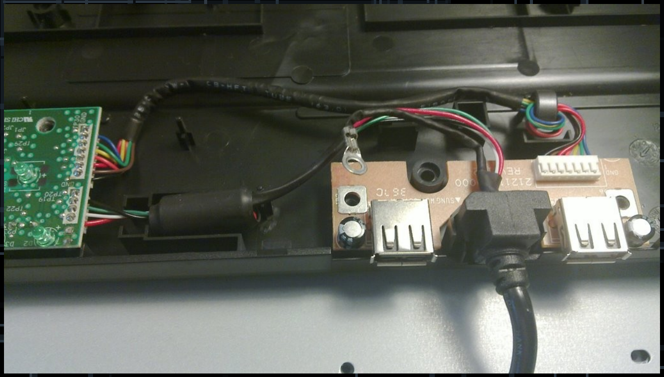
Trojan Keyboard

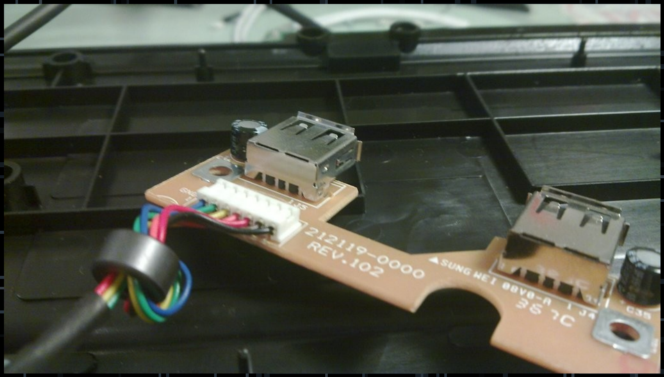
Trojan Keyboard

- Take apart the keyboard with a standard screwdriver

Trojan Keyboard

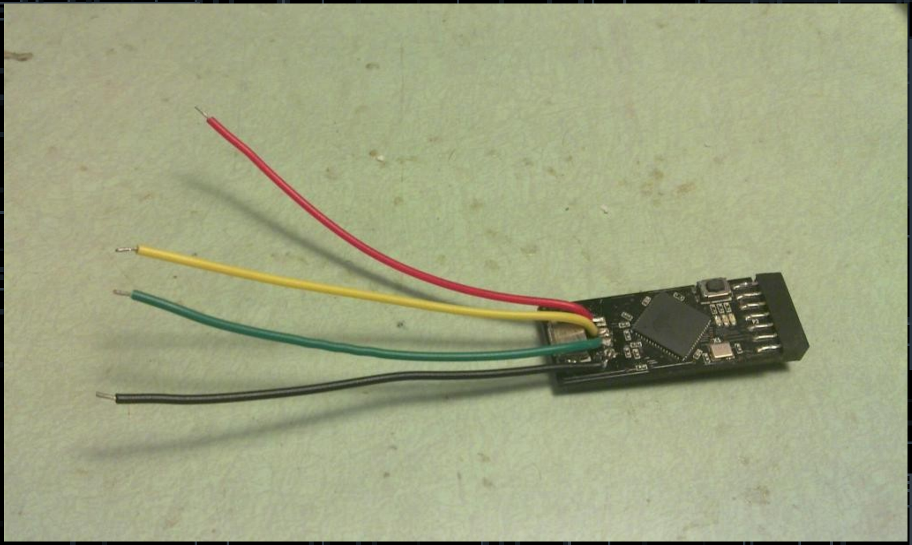
- The keyboard has an built in USB hub
- Tap in and replace one of the USB ports
- Avoid soldering by connecting into the connector with wires





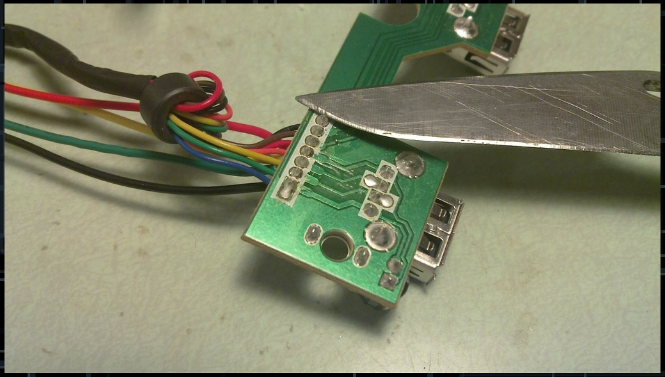
Trojan Keyboard

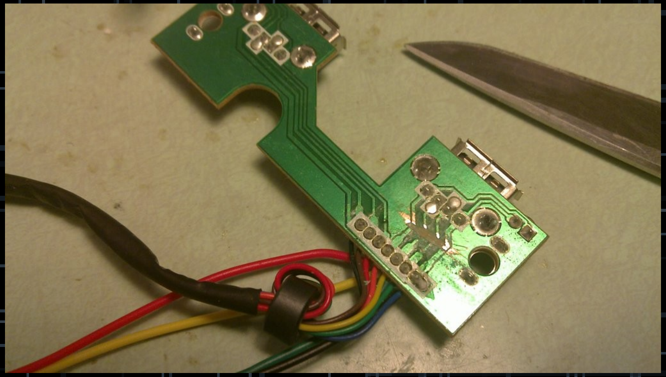
- USB cables take up to much room
- The Glitch has built in solder pads for an alternative USB connection



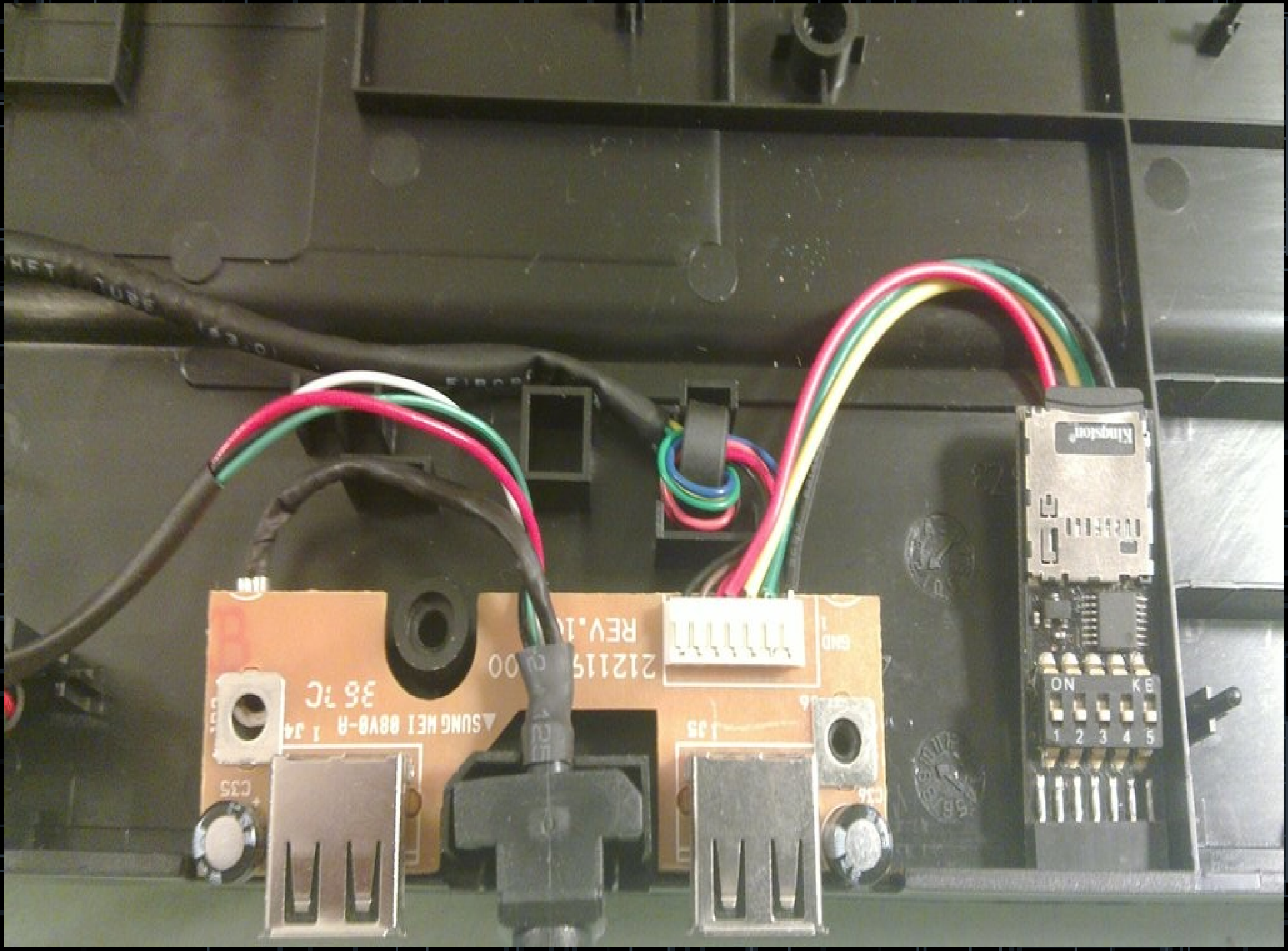
Trojan Keyboard

- Cut the lines to the USB plug
- Disables plug to avoid other device interference
    - Could also add another USB hub to keep the port active



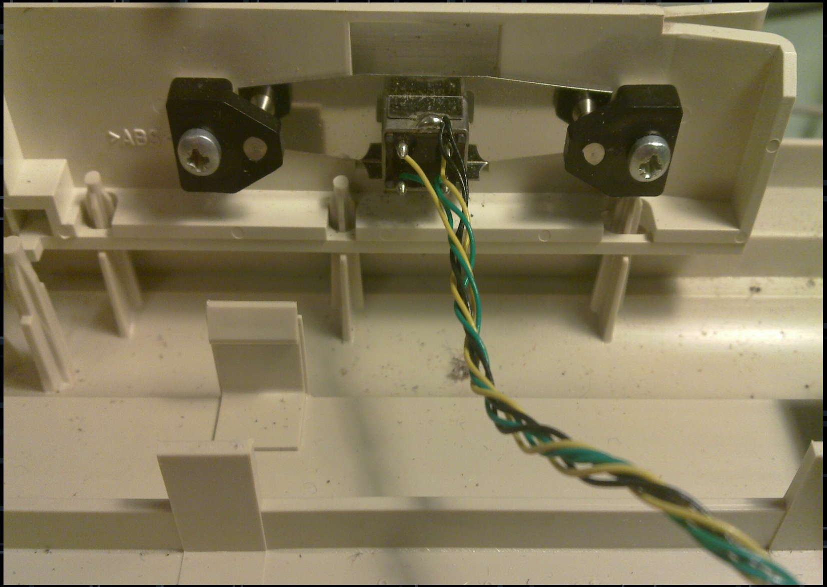


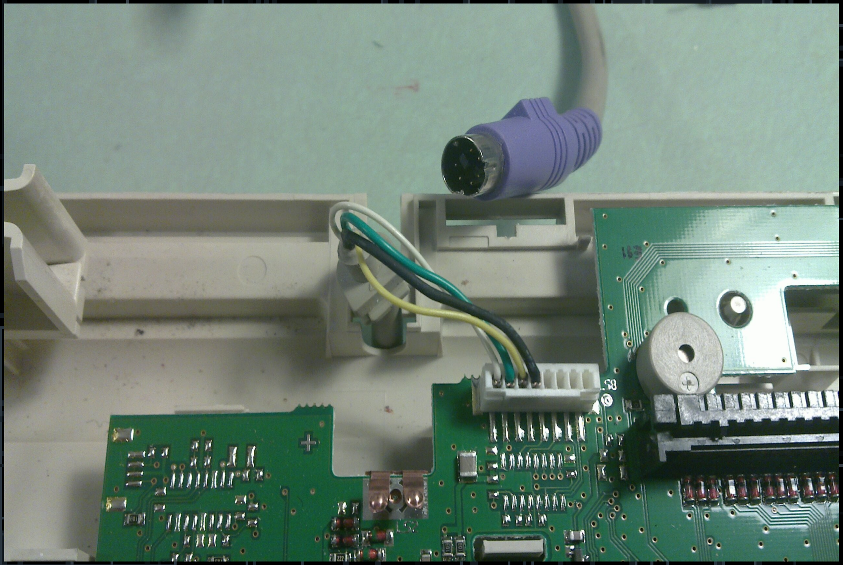
Trojan Keyboard



Trojan Card Logger

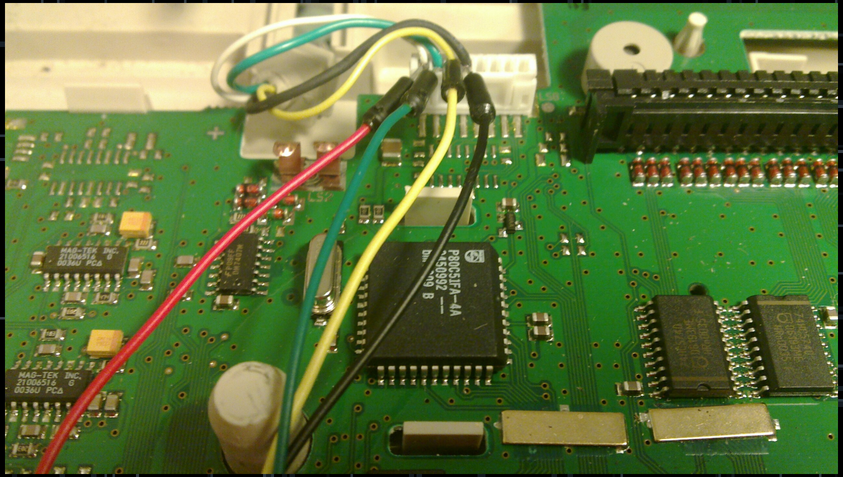
- Common PoS card reader
  - Keyboard + Mag Reader

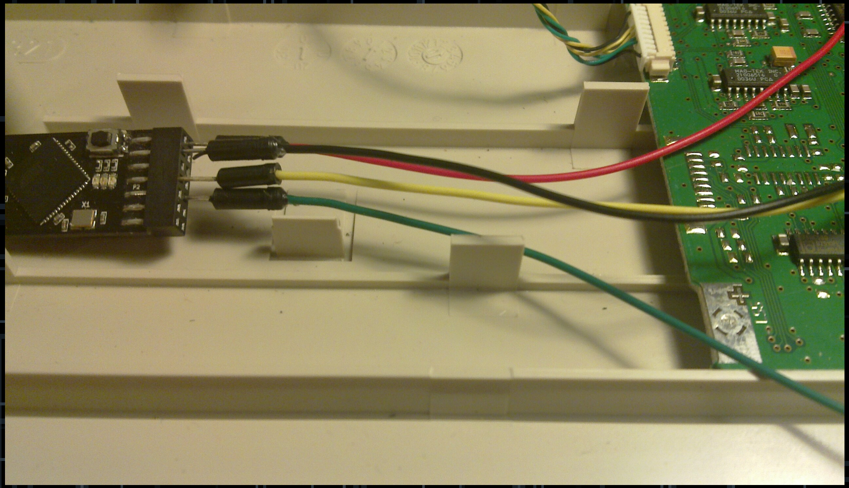




Trojan Card Logger

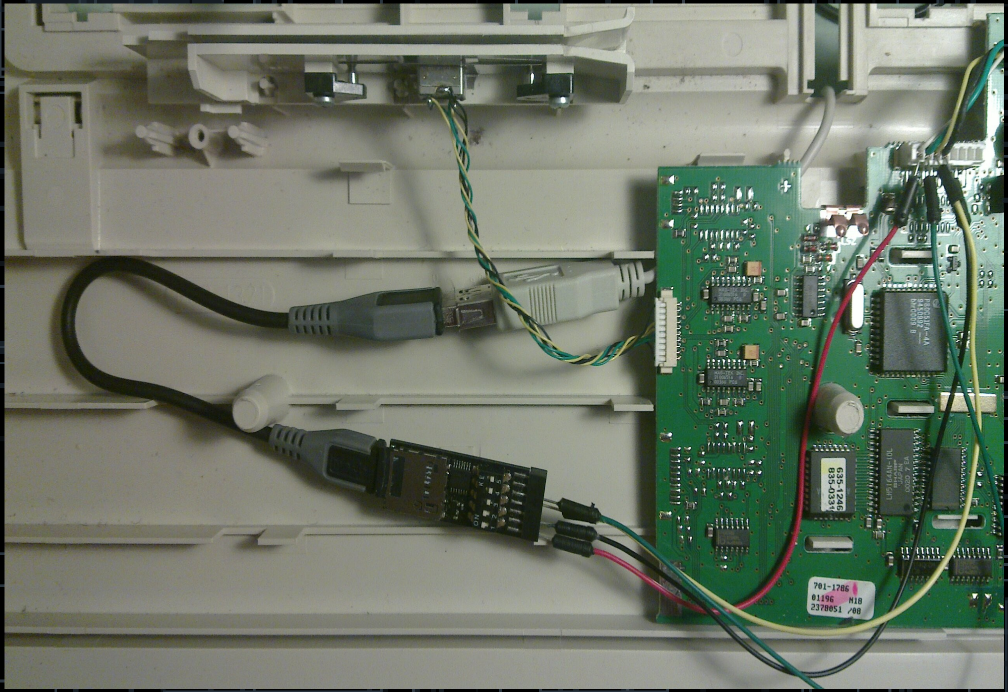
- Keyboard types card data into the PoS
- Replace the PS2 cable
- Connect to The Glitch pinouts
  - Vcc, GND,
    IRQ, DATA
- No soldering





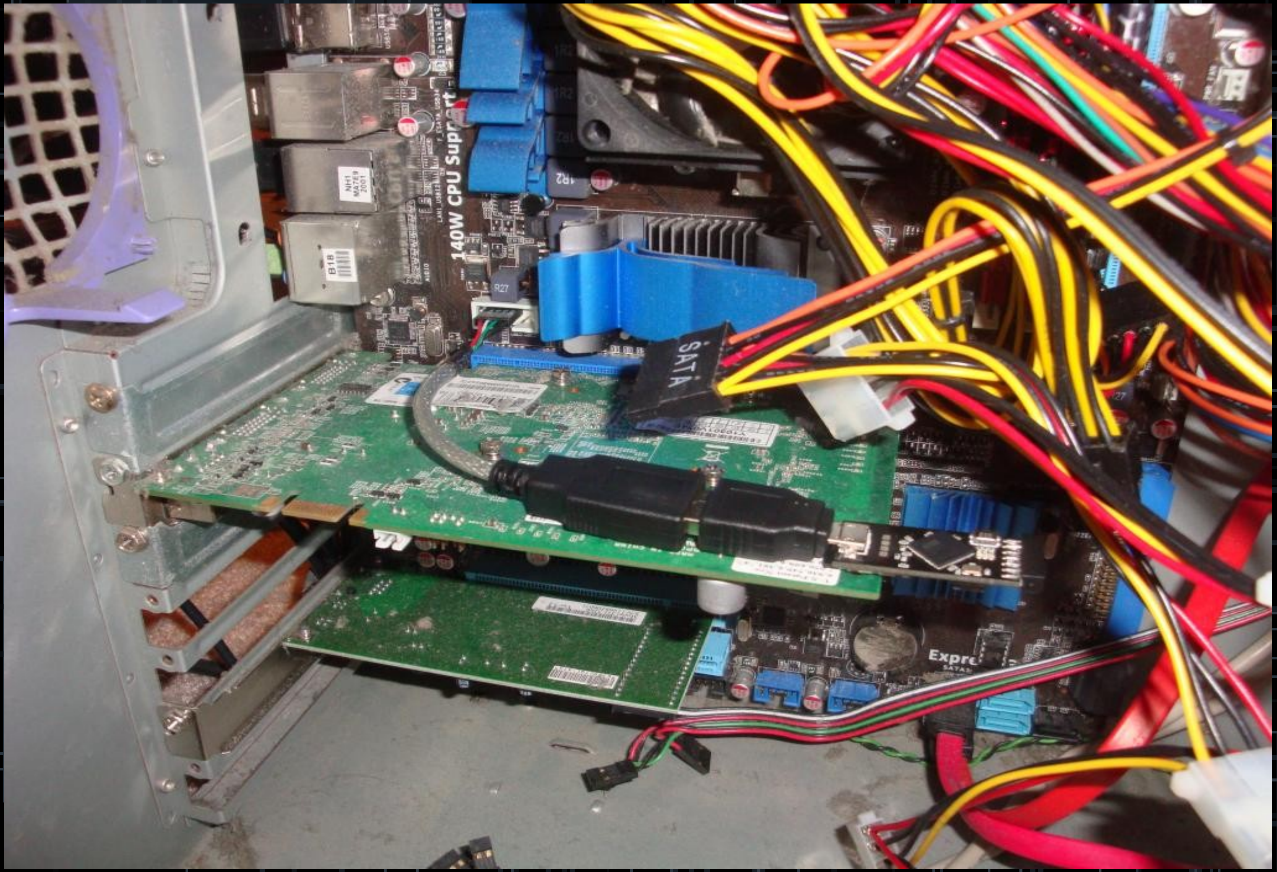
Trojan Card Logger

- Connect The Glitch USB cable to PoS
- Keystrokes converted from PS/2 to USB
- Log data on the Micro SD card



Trojan Desktop/PoS

- Plug into motherboard USB pins inside case

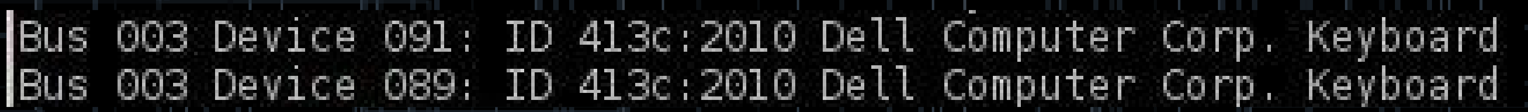


What does the User see?

- USB device drivers installing for all components
  - A few pop-ups in Windows
  - Default drivers are fine
- Launch of the attack
  - The Glitch has a new one time attack option
  - Will not attack again after each power on

How can we make this stealthier?

- Clone USB ID
  - The Glitch can clone the USB ID
  - Computer see double



```
Bus 003 Device 091: ID 413c:2010 Dell Computer Corp. Keyboard
Bus 003 Device 089: ID 413c:2010 Dell Computer Corp. Keyboard
```

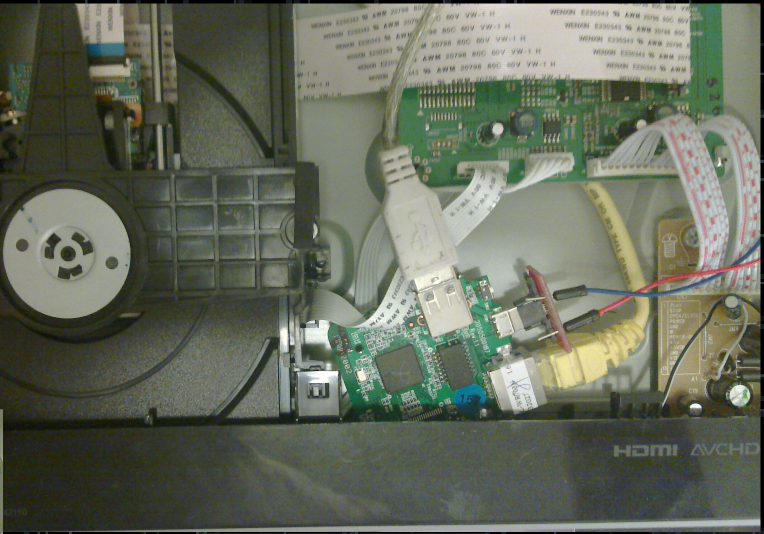
- Plan the attack
  - Make it look like an update
  - Wait a while after the Trojan device is installed

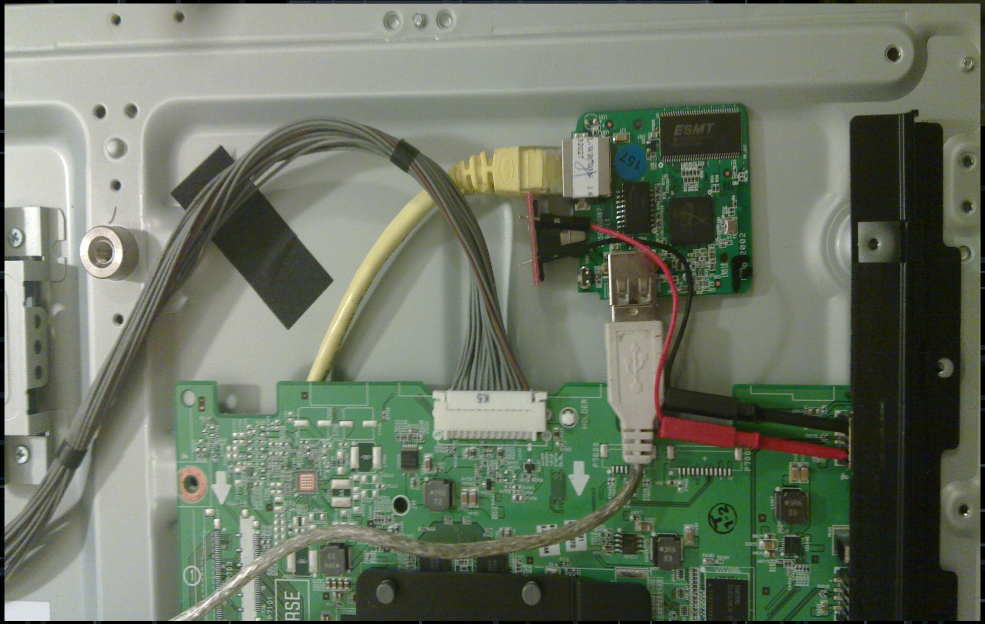
Trojan Network Connection

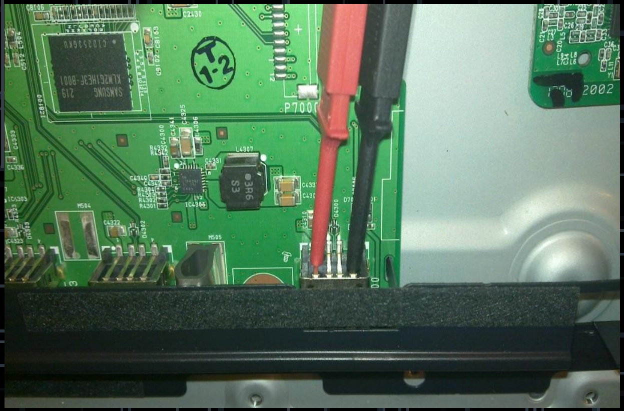
- Hardware <-> Trojan Router <-> Network
- Method
  - Remove the Ethernet connector
  - Connect PCB Ethernet headers to router
  - Connect second Ethernet cable to Ethernet connector
  - Connect USB charger to existing USB connectors on the device

Trojan LCD TV & Blu-Ray Player

- Fits in the case
- USB power and ground taps







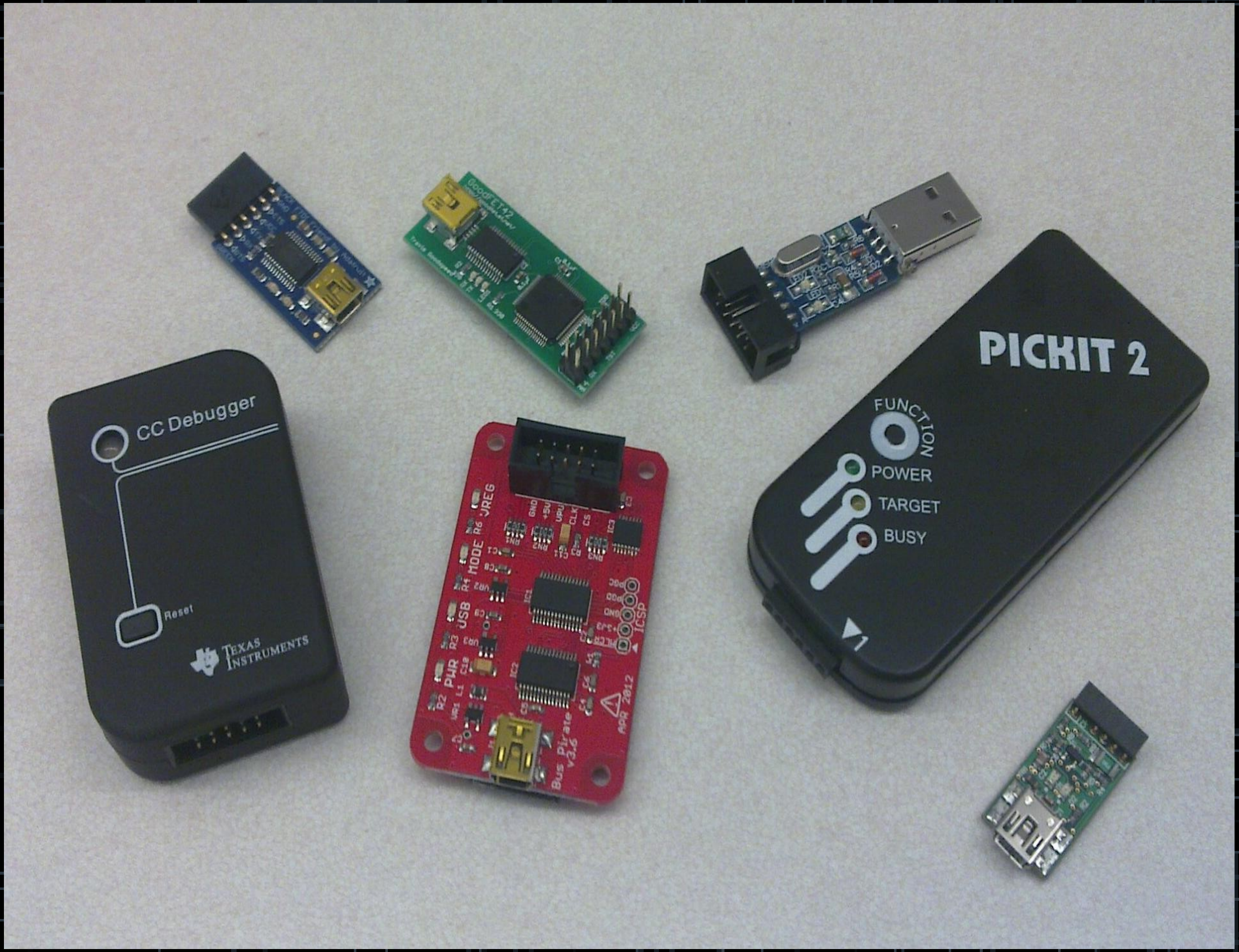
Modify Firmware

- See whats already out there about moding the device
- Research the chips
  - ARM, AVR, PIC, Texas Instrument, Broadcom, Intel, etc
- Exposed ports (or chip pin outs)
  - JTAG, UART, I2C, SPI, GPIO, etc
- Program/Debugger (often low cost)
  - Bus Pirate, Goodfet, FTDI, PICKIT, etc

Flash Firmware

- Integrated Development Environment
  - Port code or use custom language
- Look for a development community
  - Code examples
  - Custom libraries
- Flashing methods

Programmers



Customize Through Serial

- You may not need to overwrite the firmware
- Connect through a serial console over USB to UART
  - Issue AT+ commands
  - Command shell access
  - Custom commands

Linux YAY!!!

- Many mufti-function hardware platforms run Linux … YAY!!!
  - BusyBox
  - 2.4.x or 2.6.x kernel core + compiler
- Porting Linux is free and easy
  - BSD is preferred … no source code publishing required
- Compiled for custom architecture like ARM

Linux YAY!!!

- Types of devices
  - Printers
  - TVs
  - DVR/DVD/BluRay players
  - Routers
  - Watches
- PwnPlug embedded computer
- Almost anything you can ping!

Trojan Router

- Open sources router firmware
  - OpenWRT
  - DDWRT
- Replace existing router firmware on hundreds of models
  - Cisco, TP-Link, D-Link, Siemens, etc
- Configured using local Web, SSH, Telenet
- Access to underlying Linux OS
- Install / configure new applications

Trojan Router

1. Backup router web interface pages
2. Flash with open firmware
3. Integrate original web interface with open firmware
4. Configure hidden Trojan functionality
    - Enable remote VPN access
    - Create reverse SSH
    - Install hacking tools
        - MiniPwner project

Trojan Devices

Hardware Trojans

- TVs / Monitors
- Game systems
- Printers
- Mice / Keyboards
- PoS / Desktops

Firmware Trojans

- Embedded Linux
- Routers
- CC Cameras
- Controllers
- SCADA devices
- 'Internet of Things'

Ju$t l00k @R0uηd U > - <

Countermeasures

- Make purchases from a reputable source
- Monitor peripherals and network for suspicious actions
- Disable debug ports on hardware
- Enforce update authentication

Resources

- http://theglitch.sourceforge.net
- http://hackaday.com
- http://www.instructables.com/
- http://goodfet.sourceforge.net
- http://dangerousprototypes.com/docs/Bus_Pirate
- http://servicemanuals.pro
- http://minipwner.com
- http://digikey.com
- http://mouser.com

Thanks

- IronGeek, Hak5, Dave Kennedy, Dragorn, Mike Ossmann for their work in this and relating project
- Community support from Kickstarter
- BlackHat

Questions?

I have no idea what you're talking about...
...so here's a bunny with a pancake on its head.

JP Dunning ".ronin"
@r0wnin
ronin@shadowcave.org

Projects
theglitch.sourceforge.net
ww.hackfromacave.com