CyBot

Open Source Threat Intelligence Chat Bot

Tony Lee | Sr. Technical Director
(Chief Minion Herder)

TONY@CYLANCE: ~ $ WHOAMI

- **13 Years of Professional Security Experience**
  - Currently Sr. Technical Director at Cylance, Inc.
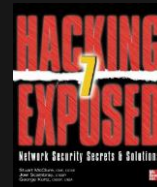- **Specialties**
  - Offensive security / Red teaming
  - Rapid prototyping and product integration
- **Education**
  - Bachelor's in Computer Engineering, Virginia Tech
  - Master's in Security Informatics, Johns Hopkins University
- **Research and Publications**
  - Contributing author to Hacking Exposed 7 and frequent blogger
  - Wireless security, China Chopper web shell, Cisco's SYNFul Knock router implant
  - Forensic Investigator Splunk app

AGENDA

INTRODUCTION

- Are you a SOC analyst or an incident responder?
- Do you get tired of pivoting to multiple tools to perform your investigation?
- Have you ever wanted a minion to do your research and bidding, but have limited time and budget?

Let CyBot be your minion!

COMPONENTS

- **Software**
  - Linux, Mac, Windows
  - Python3
  - ErrBot
  - CyBot Plugins from GitHub

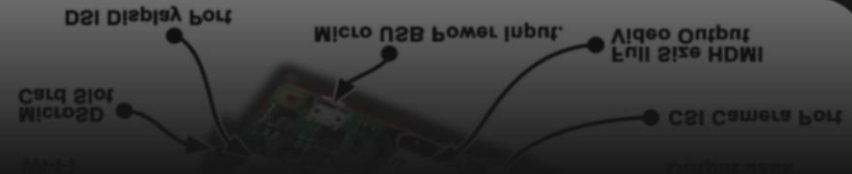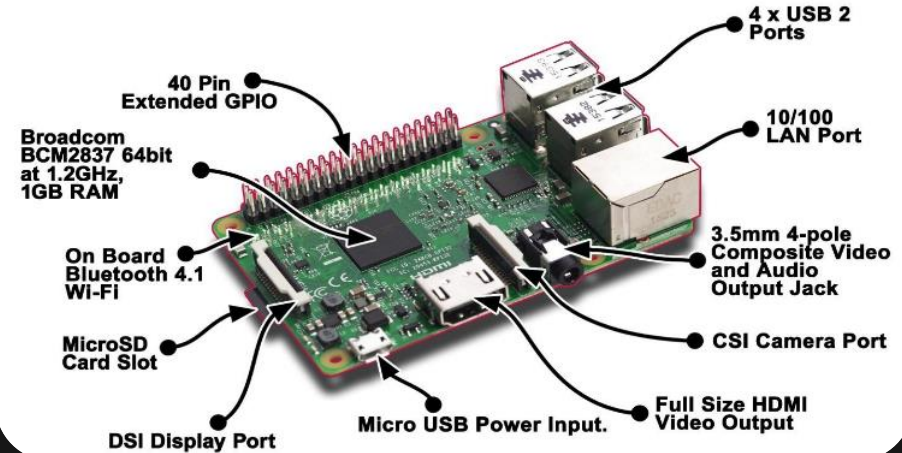
RASPBIAN

- **Hardware**
  - VM or Unused hardware that is laying around
    - -or-
  - Raspberry Pi
    - Example:
    - https://www.amazon.com/gp/product/B01CUMNIV8/ref=oh_aui_detailpage_o01_s00?ie=UTF8&psc=1

Raspberry PI 3

Wi-Fi Bluetooth

4 x USB 2 Ports

40 Pin Extended GPIO

10/100 LAN Port

Broadcom BCM2837 64bit at 1.2GHz, 1GB RAM

3.5mm 4-pole Composite Video and Audio Output Jack

On Board Bluetooth 4.1 Wi-Fi

CSI Camera Port

MicroSD Card Slot

DSI Display Port

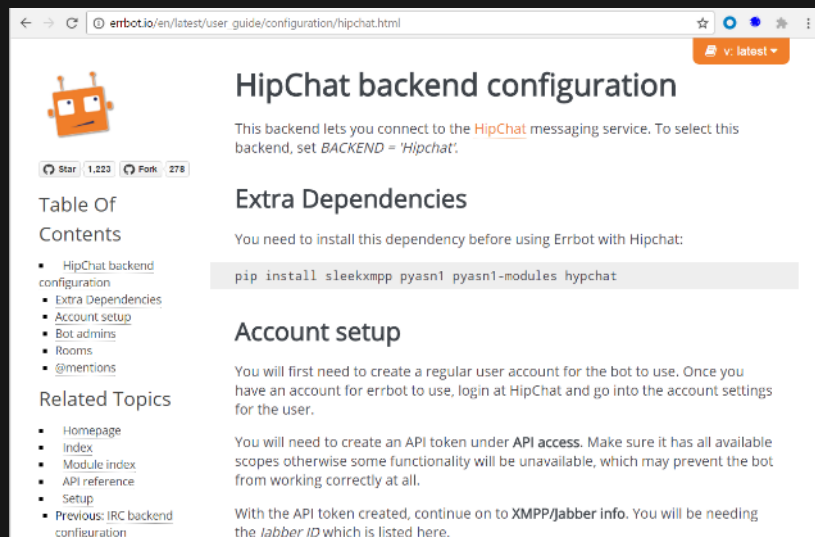Micro USB Power Input.

Full Size HDMI Video Output

COMPONENTS

- **ErrBot is very flexible and supports multiple server backends**
  - XMPP (Any standards-compliant XMPP/Jabber server should work - Google Talk/Hangouts included)
  - Hipchat
  - IRC
  - Slack
  - Telegram
  - Tox (maintained separately)
  - Gitter (maintained separately)
  - CampFire (maintained separately)
  - Skype (maintained separately)

- **Configuration largely depends on the chat protocol**
  - Our example configuration will use HipChat
  - Source: http://errbot.io/en/latest/user_guide/configuration/hipchat.html

INSTALLATION

▪ **Prerequisites**

```
sudo apt-get install python3 python-dev libssl-dev python3-pip

sudo pip3 install errbot

mkdir ~/errbot-root

cd ~/errbot-root

errbot --init
```
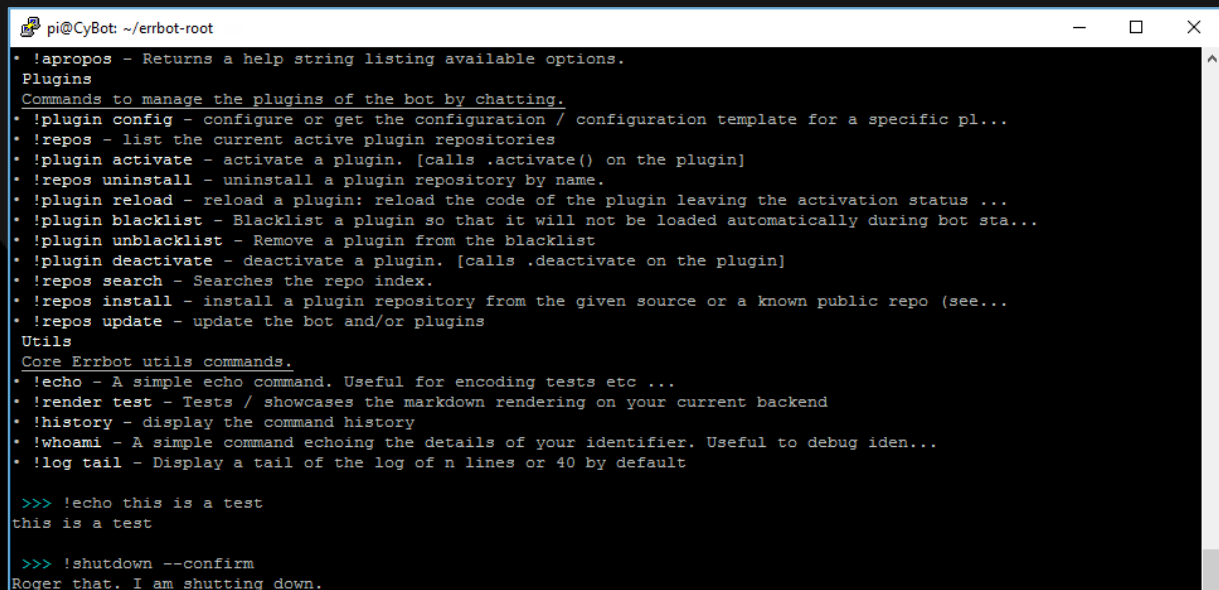
▪ **Validation**

```
errbot

!help

!shutdown --confirm
```

EXAMPLE CONFIGURATION

▪ Install ErrBot HipChat components

```
sudo pip3 install sleekxmpp pyasn1 pyasn1-modules hypchat
```

▪ Setup API user in HipChat Web UI

  ▪ Account Settings → API Access

  ▪ Create New Token

    ▪ Label: <API Label>

    ▪ Scopes:

      ▪ Select: Manage Rooms, Send Message,

        Send Notification, View Group, View Messages, View Room
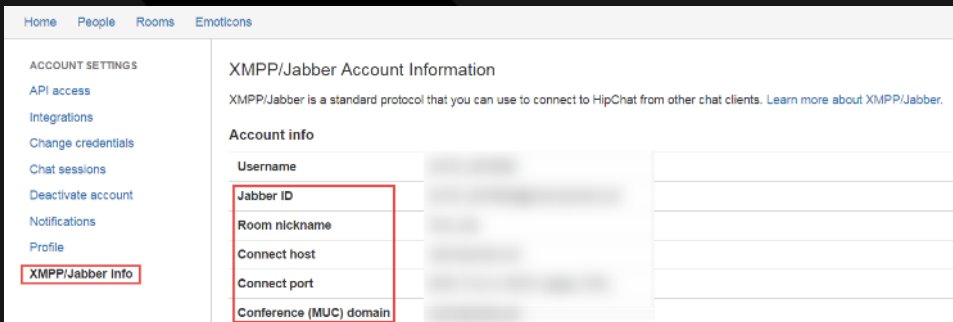
EXAMPLE CONFIGURATION

▪ Gather the following information from HipChat account settings
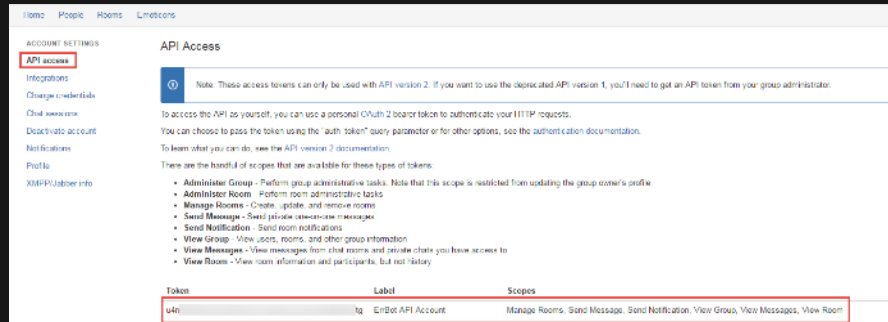
XMPP/Jabber Account Information

API token that we created

EXAMPLE CONFIGURATION

▪ Necessities for config.py

```
BACKEND = 'Hipchat'  # defaults to XMPP

BOT_DATA_DIR = r'/root/errbot-root/data'

BOT_EXTRA_PLUGIN_DIR = '/root/errbot-root/plugins'

BOT_LOG_FILE = r'/root/errbot-root/errbot.log`

BOT_LOG_LEVEL = logging.INFO


BOT_IDENTITY = {
    'username' : '12345_123456@chat.hipchat.com',
    'password' : 'changeme',
    # Group admins can create/view tokens on the settings page after logging
    # in on HipChat's website
    'token'    : 'ed4b74d628example312ff04', sleekxmpp pyasn1 pyasn1-modules hypchat
}
CHATROOM_PRESENCE = ()

CHATROOM_FN = 'CyBot'
```

EXAMPLE CONFIGURATION

▪ Added security for config.py

```
BOT_ADMINS = ('xxxxxxx@chat.hipchat.com',)

ACCESS_CONTROLS = {'status': {'allowrooms': ('someroom@conference.localhost',)},
                   'about': {'denyusers': ('*@evilhost',), 'allowrooms':
('room1@conference.localhost', 'room2@conference.localhost')},
                   'uptime': {'allowusers': BOT_ADMINS},
                   'help': {'allowmuc': False},
                   'help': {'allowmuc': False},
                   'ChatRoom:*': {'allowusers': BOT_ADMINS},
                  }

DIVERT_TO_PRIVATE = ('help', 'about', 'status', 'secnews', 'vulnnews', 'ransom', 'threat',
'aptgroup', 'cve', 'hacktool')
```

USAGE AND FEATURES

- **Control CyBot (ErrBot specific commands)**

Command	Arguments	Description
!help	N/A	Lists the help page
!room list	N/A	Lists the rooms that the bot is monitoring
!room join	XMPP room name	Joins a room to monitor
!room destroy	XMPP room name	Deletes a room – good for accidental creation
!restart	N/A	Useful for reloading plugins

- **Notes:**

  - We recommend allowing CyBot to respond to private messages in a controlled chat environment

  - CyBot must be a member of the room to respond to commands within a chat room

  - Rooms with spaces in the name require the full HipChat name

    - !room join 12345_Room_With_Space_In_The_Name@conf.hipchat.com

    - vs.

    - !room join NoSpace

Tony Lee · 8:06 AM
!room join NoSpace

CyBot · 8:06 AM
Joined the room NoSpace

USAGE AND FEATURES

▪ **Current CyBot Plugin Features**

Command	Arguments	Description
!commands	N/A	Lists all possible commands
!vt	<hash | URL>	VirusTotal Query
!hashid	<hash>	Identifies a hash type
!safebrowsing	<URL>	Google Safebrowsing Lookup
!whois	<domain or IP>	WHOIS Query
!nslookup	<domain or IP>	Forward and Reverse DNS Lookups
!geoip	<FQDN | IP>	Perform GeoIP lookup of hosts
!unshorten	<Shortened URL>	Unshorten URLs such as goo.gl and more
!linkextractor	<FQDN | IP>	Extracts links from a site
!urldecode	<URL>	Decodes an encoded URL
!unixtime	<epoch>	Convert Unix time to human readable
!codename	N/A	Generates a 2 word project codename

USAGE AND FEATURES

▪ **Example CyBot !commands menu**

Tony Lee · Jul-18 11:42 PM
!commands

CyBot · Jul-18 11:42 PM
== File commands ==

!vt <hash> - VirusTotal Query (ex: 57f222d8fbe0e290b4bf8eaa994ac641)
!hashid <hash> - Identify a hash type (e.g. MD5, SHA1) (Props: c0re)

  == Network commands ==

!vt <URL> - VirusTotal Query
!safebrowsing <URL> - Google Safebrowsing lookup (ex: ihaveaproblem.info) (Props: Google)
!whois <domain> - WHOIS Query (ex: cylance.com) (Props: hackertarget.com)
!nslookup <FQDN|IP> - DNS forward/reverse Query (ex: www.cylance.com)
!geoip <FQDN|IP> - Perform GeoIP lookup of host (ex: www.cylance.com) (Props: freegeoip.net)
!unshorten <shortened URL> - Unshortens URLs (ex: goo.gl/IGL1IE)
!linkextractor <FQDN|IP> - Extracts links from a site and safely displays them (ex: hxxps://www.google.com)
!urldecode <url> - Decodes encoded URLs (ex: /%75%72%6C?%73%61=%74)

  == Misc ==

!unixtime <epoch> - Convert Unix time to human readable (ex: 1347517370)
!codename - Generates a 2 word project codename (Props: Mark Biek)
Show less

RELEASED AT BLACK HAT EUROPE 2017

▪ **New CyBot Plugin Features**

Command	Arguments	Description
!secnews	N/A	Displays latest cyber security news
!vulnnews	N/A	Displays latest computer vulnerability news
!time	<timezone>	Query time in specified timezone
!weather	<zipcode>	Query the weather in a specified zip code
!calc	<arithmetic input>	Performs basic arithmetic (Valid input: [0-9]+-/) (ex: 22*3)
!bitcoin	N/A	Polls the latest Bitcoin Price Index (BPI)

RELEASED AT BLACK HAT ASIA 2018

▪ **New CyBot Plugin Features**

Command	Arguments	Description
!wintime	<epoch>	Convert Windows time (100-nanosecond intervals since January 1, 1601) to human readable (ex: 131580340430000000)
!joke	N/A	Queries an on-line API repository of jokes (Props: icanhazdadjoke)
!ransom	<keyword>	Indentify ransomware by searching the Ransomware Overview Spreadsheet (Props: http[:]//goo[.]gl/b9R8DE)
!stats	<YYYY or YYYY-MM or YYYY-MM-DD>	Produce usage statistics for a day or month (ex: 2017-12)
!cc	<Credit Card Number>	Tests validity of a CC number and attempts to determine the brand (ex: 4012888888881881 or 378282246310005)
!uastring	<User Agent String>	Determines the victim operating system and browser based on the user agent string

RELEASED AT BLACK HAT USA 2018

▪ **New CyBot Plugin Features**

Command	Arguments	Description
!cve	<#>	Return the last n CVE's (Props: CIRCL https[:]//www[.]circl[.]lu).
!aptgroup	<search string>	Retrieve information on common APT groups (Props: huntoperator)
!hacktool	<search string>	Retrieve information on common hacking tools (Props: huntoperator)
!threat	<search string>	Search APT group activity mapped to MITRE ATT&CK Framework (Props: huntoperator)

▪ **Updated**

Command	Arguments	Description
!geoip	<FQDN|IP>	Perform GeoIP lookup of host (ex: www[.]cylance[.]com) (Props: ip-api[.]com)

RELEASING AT BLACK HAT EUROPE 2018

▪ **Upgraded and Improved Functionality CyBot Plugin Features**

Command	Arguments	Description
!cve	<# | ####-####>	Return the last n CVE's or a specific CVE (Props: CIRCL https[:]//www[.]circl[.]lu).
!aptgroup	<search string>	Retrieve information on common APT groups (Props: huntoperator)
!hacktool	<search string>	Retrieve information on common hacking tools (Props: huntoperator)
!threat	<search string>	Search APT group activity mapped to MITRE ATT&CK Framework (Props: huntoperator)
!ransom	<search string>	Indentify ransomware by searching the Ransomware Overview Spreadsheet (Props: http[:]//goo[.]gl/b9R8DE)

▪ **Command Injection Bug Fix**

Command	Arguments	Description
!hashid	<hash>	Identifies a hash type

OUTPUT IMPROVEMENTS

BUG DETAILS – PROBLEM & SOLUTION

```
cat hashid.py

...

class hashid(BotPlugin):

    @arg_botcmd('hash', type=str)   # flags a command

    def hashid(self, msg, hash=None):

        dir_path = os.path.dirname(os.path.realpath(__file__))

        cmd = dir_path + "/hashidentifier.py " + hash

        output=os.popen(cmd).read()

        return(output)
```

```
>>> !hashid foo;"uname -a"
Analyzing 'foo'
[+] Unknown hash
:                                         SMP Fri Aug 11 21:17:51

>>> !hashid foo;whoami
Analyzing 'foo'
[+] Unknown hash
user

>>> !hashid foo;"cat /etc/passwd"
Analyzing 'foo'
[+] Unknown hash
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

```
if not re.findall(r"(^[a-fA-F\d]+$)", hash):

        # Input may contain illegal characters

        return("Your submission may contain characters not
ordinarily found in hashes.  Please try again or contact
the developer if you believe this to be an error.")
```

```
>>> !hashid foo;"uname -a"
Your submission may contain characters not ordinarily found in hashes.

>>> !hashid foo;whoami
Your submission may contain characters not ordinarily found in hashes.

>>> !hashid foo|"cat /etc/passwd"
Your submission may contain characters not ordinarily found in hashes.
```

Huge thanks to Jake Valletta (@jake_valletta) for caring and for responsible disclosure!

DEVELOPMENT

- Always on-going
- Roadmap is robust
  - Automated report writing
  - SIEM integration
  - Ticketing system integration
- Open to everyone as a community project
- Plugins written in Python
- Plugins are chat backend agnostic and will work with all platforms supported by errbot
- Code contributions go to GitHub
- New ideas welcomed!

PRO TIPS

- If installed on Raspberry Pi

  - Set a static IP

    - sudo leafpad /etc/dhcpcd.conf   (at the end enter)

    ```
    interface eth0
    static ip_address=<ip.ad.dr.ess>
    static routers=<ip.ad.dr.ess>
    static domain_name_servers=<ip.ad.dr.ess>
    ```

  - You may need to set US (or other regional) keyboard since this defaults to UK
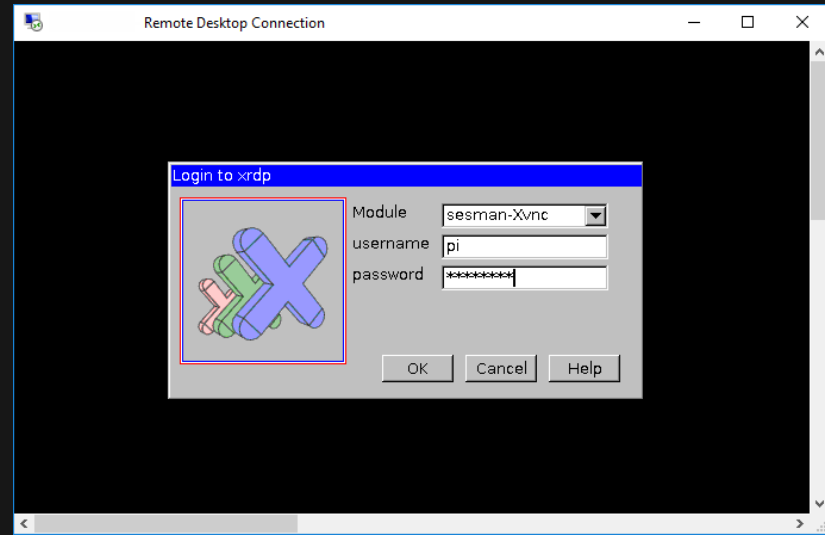
    - "Start" -> Preferences -> Mouse and Keyboard Settings -> Keyboard tab -> Keyboard Layout -> United States -> English (US)

  - Install remote desktop

    - sudo apt-get install vnc4server

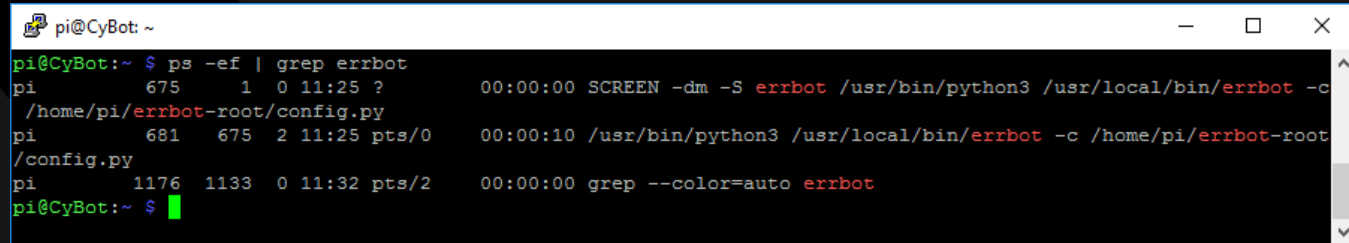   - sudo apt-get install xrdp

  - Set SSH to autorun on boot

    - sudo update-rc.d ssh enable

PRO TIPS

- If installed on Raspberry Pi (cont.)
  - Set errbot to autorun on boot in a detached screen session
    - sudo apt-get install screen
    - sudo leafpad /etc/rc.local
    - Add the following line before the "exit 0" line:
    - su - pi -c "screen -dm -S errbot /usr/bin/python3 /usr/local/bin/errbot -c /home/pi/errbot-root/config.py"
  - Interact with the screen session by using: "screen -d -r"
  - Adjust screensaver settings easily (this will place a shortcut in preferences):
    - sudo apt-get install xscreensaver
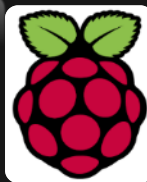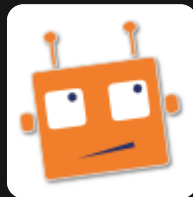
ACKNOWLEDGEMENTS

- **Platform:**
  - ErrBot - http://errbot.io/en/latest/
  - Raspberry Pi - https://www.raspberrypi.org/

- **Plugins:**
  - VirusTotal - https://www.virustotal.com/
  - GeoIP – ip-api-com
  - Google – safe browsing, news feeds
  - Hashid – c0re
  - Unshorten – unshorten.me
  - Many more…

- **People:**
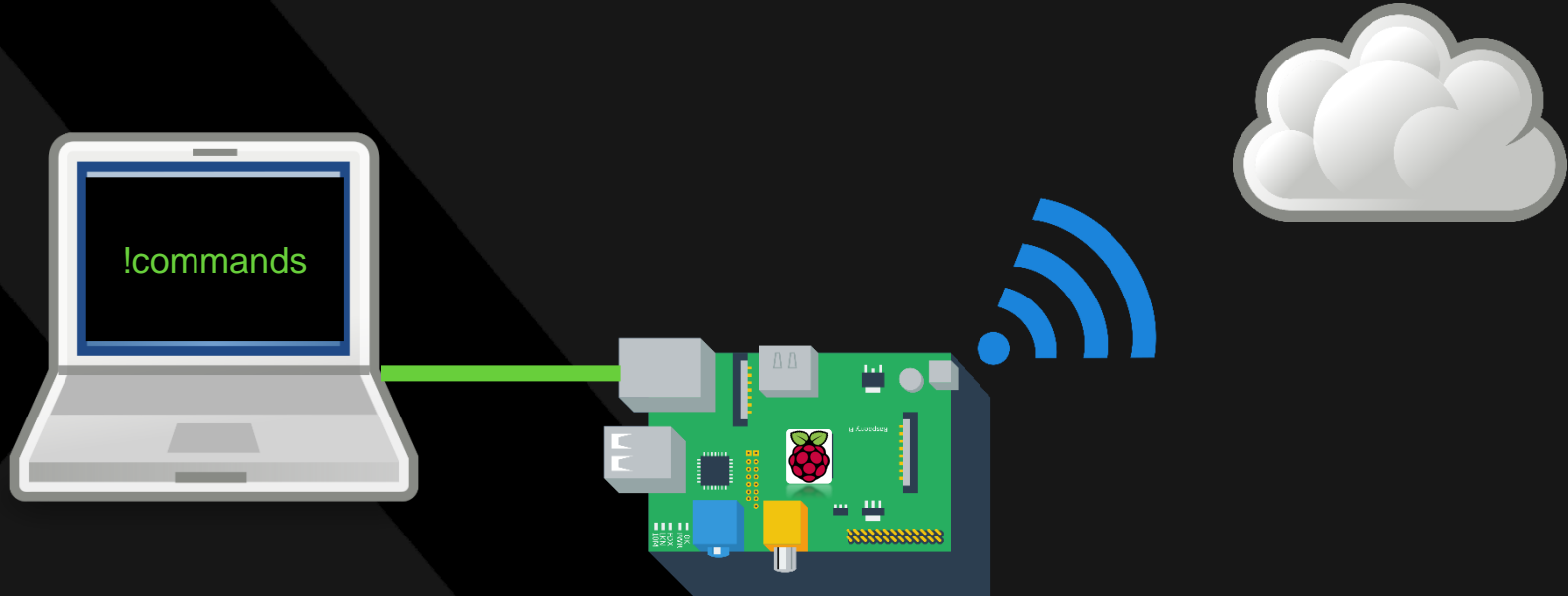 - Bill Hau, Corey White, Dennis Hanzlik, Ian Ahl, Dave Pany, Dan Dumond, Kyle Champlin

DEMO!

!commands

QUESTIONS

AND

ANSWERS

Thank you

BACKUP SLIDE IN CASE LIVE DEMO TANKS

```
 >>> !geoip www.google.com
"ip":"2607:f8b0:4006:81b::2004"
"country_code":"US"
"country_name":"United States"
"region_code":""
"region_name":""
"city":""
"zip_code":""
"time_zone":""
"latitude":37.751
"longitude":-97.822
"metro_code":0
```

```
 >>> !hashid 57f222d8fbe0e290b4bf8eaa994ac641
Analyzing '57f222d8fbe0e290b4bf8eaa994ac641'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
--snip--
```

```
 >>> !safebrowsing ihaveaproblem.info
{'matches': [{'threatEntryType': 'URL', 'cacheDuration': '300s', 'threat': {'url': 'ihaveaproblem.info'},
'threatType': 'SOCIAL_ENGINEERING', 'platformType': 'ANY_PLATFORM'}]}
```