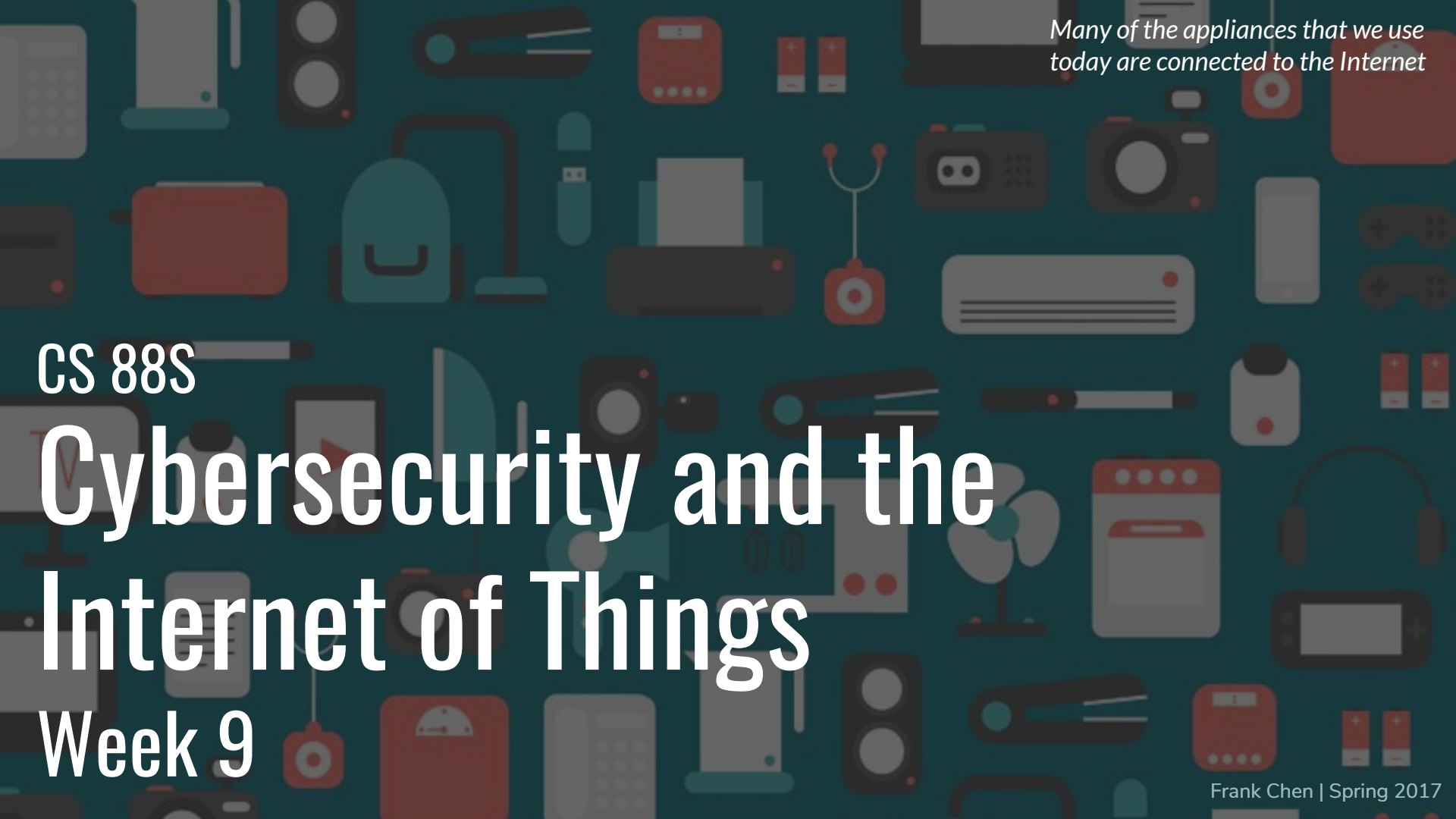


Many of the appliances that we use today are connected to the Internet

CS 88S

Cybersecurity and the Internet of Things

Week 9

Frank Chen | Spring 2017

Agenda

- *Review week 7's material*
- *Smart Transportation*
- *Healthcare Devices*
- *Smart Assistants*
- *Home Appliances*
- *MIRAI DDoS Attack*

Agenda

- ***Review week 7's material***
- *Smart Transportation*
- *Healthcare Devices*
- *Smart Assistants*
- *Home Appliances*
- *MIRAI DDoS Attack*

Tech Companies or Ad Companies?

"Mobile now makes up 84 % of ad revenue"

Source: http://tcrn.ch/2ktzjFU

"Alphabet's revenue hit $21.5 billion, a 21 percent year-over-year increase. Of that revenue, $19.1 billion came from Google's advertising business"

Source: http://bit.ly/2rf5Boe

Amazon Go's 3 Steps

Make a video

Get the Patents

Prove then Wait

Source: http://bit.ly/2iBsBxh

The Invisibility Cloak

Image Source: http://bit.ly/2qZpIKA

A Cool Demo from CTF

Agenda

- *Review week 7's material*
- ***Smart Transportation***
- *Healthcare Devices*
- *Smart Assistants*
- *Home Appliances*
- *MIRAI DDoS Attack*

Jeep Cherokee

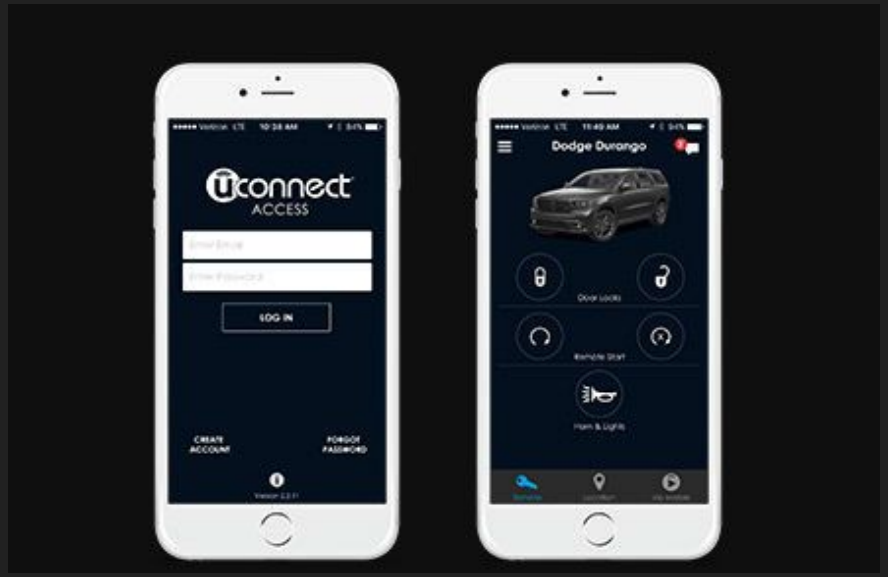
Source: jeep.com

Remote Jeep Hack

- *Zero-day exploit on Jeep Cherokees*
- *Attackers obtain wireless control, via the Internet, to any Jeep Cherokees*

For detailed explanation of the hack: http://bit.ly/2rdUL2Q

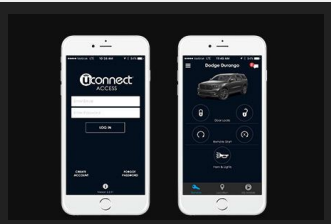
UConnect



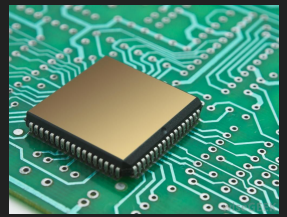
Source: http://bit.ly/1ZcoZgH

Hack Outline

Exploit *UConnect's vulnerability to gain access*



Rewrite *Entertainment Hardware Chip Firmware*



Send *commands through CAN bus to car's physical components (engines, wheel)*

Source: http://bit.ly/1ZcoZgH

Steer Fast!

Source: http://bit.ly/2aIa3ae

Remote Jeep Hack

Chrysler has issued a recall for 1.4 million vehicles as a result of Miller and Valasek's research.

The Message:

Automakers need to be held accountable for their vehicles' ***digital security.***

Source: http://bit.ly/1ZcoZgH

Agenda

- *Review week 7's material*
- *Smart Transportation*
- ***Healthcare Devices***
- *Smart Assistants*
- *Home Appliances*
- *MIRAI DDoS Attack*

Source: viastara.com

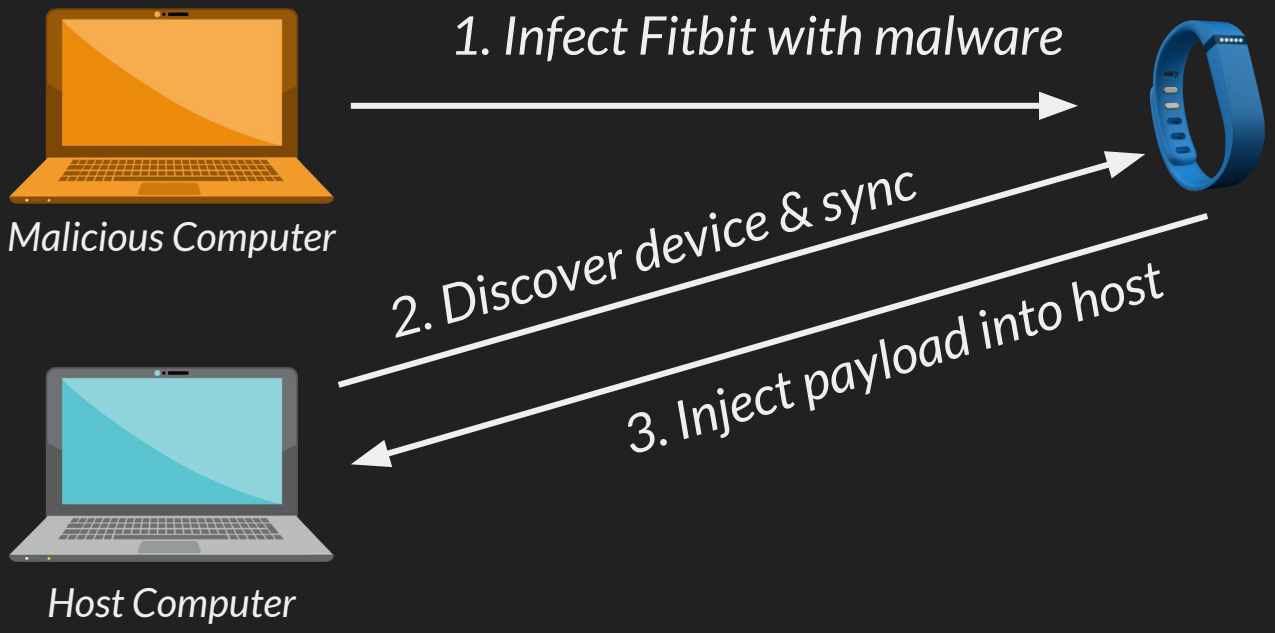
Fitbit Data Dump

"Cybercrime takes many forms, but one of the more insidious and perhaps less obvious manifestations is warranty fraud"

- Brian Krebs

Source: http://bit.ly/1nd7QGu

Fitbit Hacked



Source: http://bit.ly/2r5xfqq

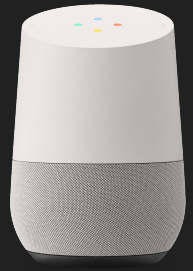
Agenda

- *Review week 7's material*
- *Smart Transportation*
- *Healthcare Devices*
- ***Smart Assistants***
- *Home Appliances*
- *MIRAI DDoS Attack*

Source: qz.com

How many are there?

Amazon Alexa



Google Home

Siri

Hi, I'm Cortana.

Alexa Demo

Source: qz.com

Incidents

- *Dollhouse Incident (`http://bit.ly/2iUuaWW`)*
- *Connectivity Issues (`http://bit.ly/2fwb2L7`)*
- ***Amazon Alexa Murder Case** (http://bit.ly/2luUdlK)*

Preview for next week...

"Do you have to give informed consent to be recorded each time you enter my Alexa-outfitted home?"

Source: http://bit.ly/2luUdlK

Preview for next week...

*"Google will share your information with companies, organizations, and individuals outside of Google if Google has a good-faith belief that access, use, preservation, or disclosure of the information is **reasonably necessary** to meet applicable law, regulation, legal process, or enforceable government request."*

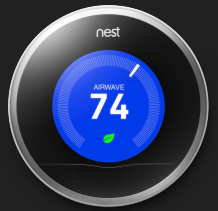
Source: http://bit.ly/2luUdlK

Agenda

- *Review week 7's material*
- *Smart Transportation*
- *Healthcare Devices*
- *Smart Assistants*
- ***Home Appliances***
- *MIRAI DDoS Attack*

Source: nest.com

Appliances



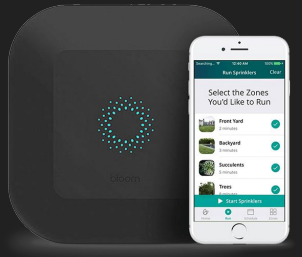
Nest Thermostat

Samsung Smart Fridge

Wink, TCP connected lighting system

August, smart door lock

Lorex Home Security



Blossom, smart water sprinkler

Secure? Or nah

Source: http://bit.ly/2mkgTtn

Security Issues

- *Confidential Information*
- *Monetary Damage*
- *Physical Danger*

Source: wired.com

Agenda

- *Review week 7's material*
- *Smart Transportation*
- *Healthcare Devices*
- *Smart Assistants*
- *Home Appliances*
- ***MIRAI DDoS Attack***

Source: wired.com

Review: DDoS Attack

Source: wired.com

Accessibility

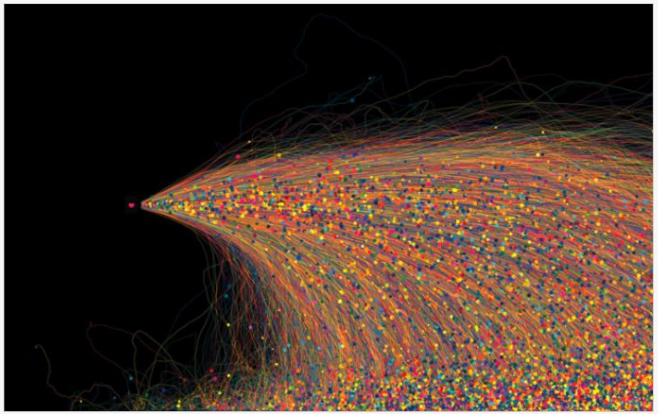
C

I

A

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Posted Oct 21, 2016 by Darrell Etherington (@etherington), Kate Conger (@kateconger)



Several waves of major cyberattacks against an internet directory service knocked dozens of popular websites offline today, with outages continuing into the afternoon.

Twitter, SoundCloud, Spotify, Shopify, and other websites have been inaccessible to many users throughout the day. The outages are the result of several distributed denial of service

Crunchbase

Twitter –

FOUNDED
2006

OVERVIEW
Twitter is a global social networking platform that allows its users to send and read 140-character messages known as "tweets". It enables registered users to read and post their tweets through the web, short message service (SMS), and mobile applications. As a global real-time communications platform, Twitter has more than 400 million monthly visitors and 255 million monthly active users around ...

LOCATION
San Francisco, CA

CATEGORIES
SMS, Blogging Platforms, Social Media, Messaging

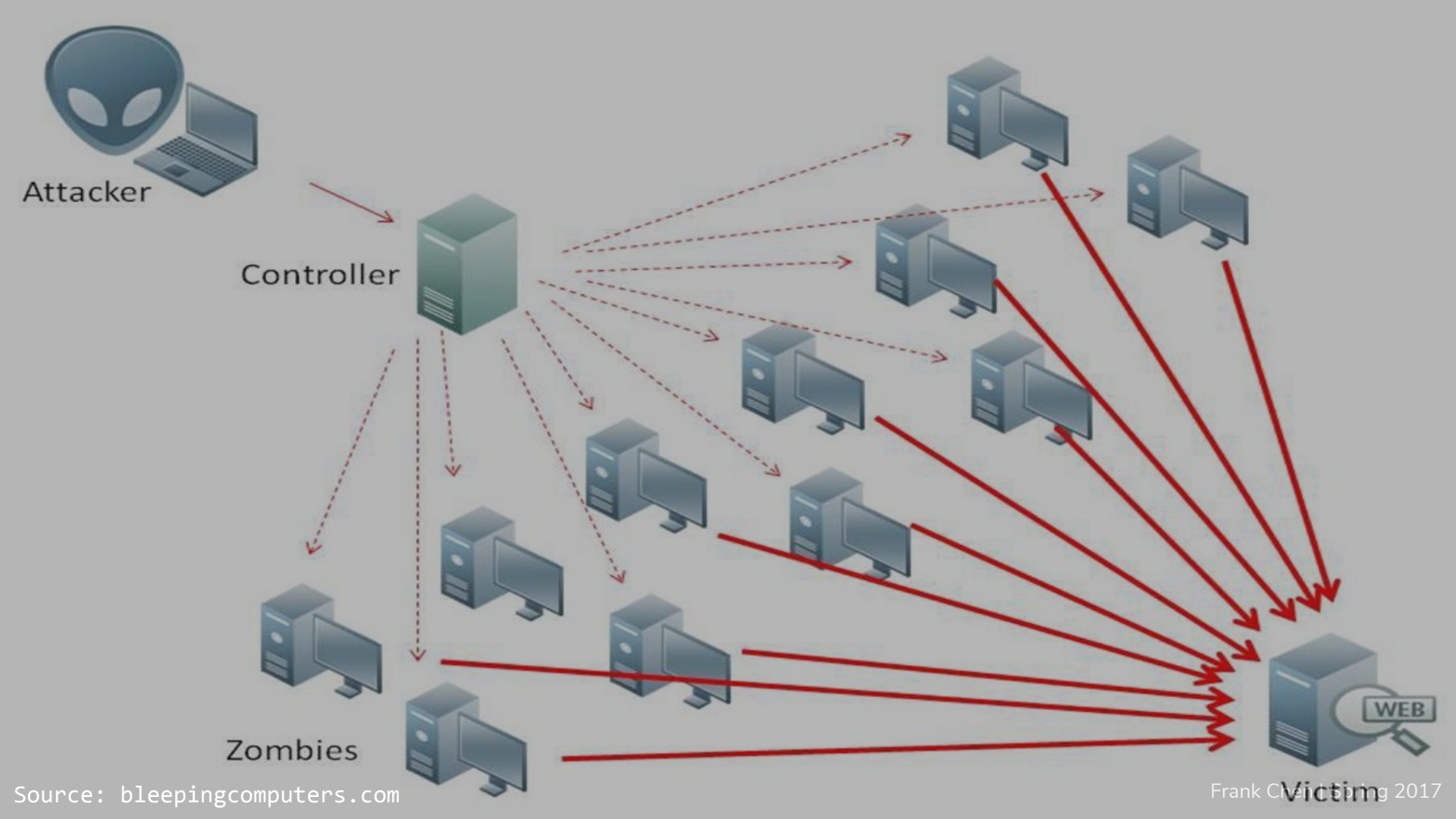
WEBSITE
http://www.twitter.com/

Full profile for Twitter

Spotify +

Shopify +

http://tcrn.ch/2dt8sHy



Source: bleepingcomputers.com

Timeline of Events

First attack began at 7:00am (EDT)

A second attack was reported at 11:52am and Internet users began reporting difficulties accessing websites

At 6:11pm, Dyn reported that they had resolved the issue

Resolved by 9:20am

A third attack began in the afternoon, after 4:00pm

October 21, 2016

Source: krebsonsecurity.com

Affected Websites

The MIRAI Virus

- *Call-Home System*
  - *connects to a command-and-control server (which could be another insecure IoT device) to download details of whom to attack, and how.*
- *Set of Attack Routines*
  - *generate a range of legitimate-looking streams of network traffic to eat away at the victim's network capacity.*
- *Network Scanner*
  - *searches on the internet & try to login in various ways to build and report a list of insecure IoT devices for the next wave of attacks.*

Source: http://bit.ly/2dLMyev

The MIRAI Virus

Open Source: *https://github.com/jgamblin/Mirai-Source-Code*

Source: http://bit.ly/2dLMyev

The **MIRAI** Virus

Written in Go for ***Cross-Platform Support***

Source: http://bit.ly/2dLMyev

The MIRAI Virus

Uses built-in default passwords...

root/xc3511	root/vizxv	root/admin
admin/admin	root/888888	root/xmhdipc
root/default	root/juantech	root/123456
root/54321	support/support	root/(none)
admin/password	root/root	root/12345
user/user	admin/(none)	root/pass
admin/admin1234	root/1111	admin/smcadmin
admin/1111	root/666666	root/password
root/1234	root/klv123	Administrator/admin
service/service	supervisor/supervisor	guest/guest
guest/12345	guest/12345	admin1/password
administrator/1234	666666/666666	888888/888888
ubnt/ubnt	root/klv1234	root/Zte521
root/hi3518	root/jvbzd	root/anko
root/zlxx.	root/7ujMko0vizxv	root/7ujMko0admin
root/system	root/ikwb	root/dreambox
root/user	root/realtek	root/00000000
admin/1111111	admin/1234	admin/12345
admin/54321	admin/123456	admin/7ujMko0admin
admin/1234	admin/pass	admin/meinsm
tech/tech	mother/fu[redacted]r	

Mirai's built-in password dictionary.

Source: http://bit.ly/2dLMyev

Recommendations

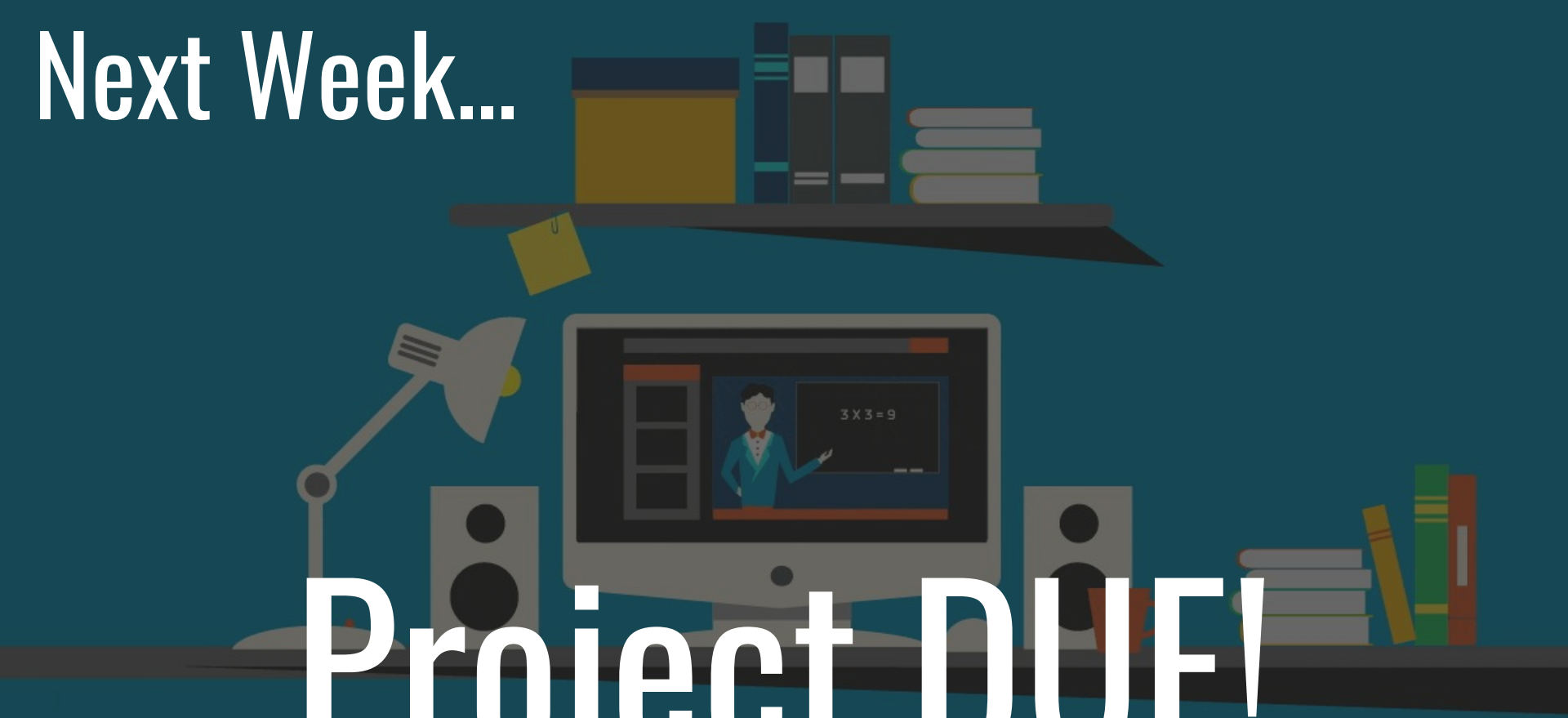
- *Don't use hardwired passwords*
- *Don't set default passwords*
- *Don’t allow unauthenticated or unencrypted protocols for inbound connections*
- *Don’t open administrative connections on the outside interface by default.*

Source: http://bit.ly/2dLMyev

Safety in the Cloud Tip

Do not use default password and username in IoT devices.

Next Week...



Project DUE!

Image Source: http://bit.ly/2pIoWQW


PANDORA'S iPHONE
BACK DOOR
FBI
APPLE
HACKERS
REPRESSIVE REGIMES
ETC.

Next Week...