IoT THIS WEEK

Episode 24

April 17, 2017

Catching you up on the latest from IoT, InfoSec and Tech. Episode 24 includes: Mirai mines bitcoin, IoT maker disconnects customer, Bricker Bot says no more IoT for you, a spammer gets arrested and much more...

IoT

I've made some changes to Firmwalker on Github. In addition to getting the serial number of a *.crt file by running against OpenSSL, I'm also running that serial number against Shodan using the Shodan CLI. Have a look.

Mirai can now mine bitcoin. A new version is able to conduct DDoS attacks and mine bitcoin. It a really interesting story on how IBM detected and noticed what the new version was doing.

11 states now considering "Right to Repair" bills. Iowa, Missouri and North Carolina joined eight other states in introducing legislation to allow people to repair the devices they have bought. So far it looks like the bills will be defeated in Minnesota and Nebraska. Tennessee deferred to 2018 and bills are still pending in New York, Massachusetts, Illinois, Kansas, Wyoming, Iowa, Missouri and North Carolina.

Connected IO launches a miniature modem for IoT. The modem is designed to take advantage of the low latency broadband cellular network known as 'Cat 1". The modem devices are not much larger than a computer chip and are designed to transfer small amounts of data on narrow bandwidth. Similar devices already allow Coca-Cola to determine when their vending machines will run out of stock.

IoT maker bricks customer's garage door on purpose. Garadget remotely denied service to back-end servers from a customer's Wi-Fi garage door for giving a bad review on Amazon. The device connection was ultimately restored after the owner admitted disabling the device may have been a bad move.

IoT malware showing destructive behavior. New malware identified by Palo Alto Networks named Amnesia is infecting digital video recorders through a year old vulnerability. Amnesia is a variation of Tsunami. The new malware also tries to determine if it is running inside a virtual environment. Basically it's trying to determine if it's running in a honeypot. If it thinks it is in a virtual environment, it attempts to wipe files by using "rm -rf".

BrickerBoT renders IoT devices useless. Radware identified the malware which accesses devices by brute forcing username/password. It then attempts to use commands available in Busybox to write random data to any drives. A new name for this has been coined: Permanent Denial-of-Service (PDoS).

Startup wants to build a nano satellite fleet for IoT. The fleet would consist of 100 nano satellites. Nano satellites are currently used for things like Earth observation and mapping. In addition to 5G mobile networks, this would be another avenue for helping IoT devices to communicate.

McAfee says 2.5 million IoT devices infected with Mirai botnet in Q4 2016. The McAfee Labs Threats Report April 2017 notes that five IoT device IP addresses are infected by the Mirai botnet each minute.

InfoSec

Microsoft patching Office zero day on patch Tuesday. The vulnerability affects the Windows' Object Linking and Embedding (OLE) which lets users embed or link to other Office documents.

Detailed write-up on exploiting Broadcom's Wi-Fi Stack. This details a remote code execution exploit giving someone control over Broadcom's Wi-Fi SoC.

DNS record will soon help prevent unauthorized SSL certificates. In several months public certificate authorities will be required to start honoring a DNS record that allows domain owners to specify who is allowed to issue SSL certificates for their domain. So once this record is in place, you can basically say that only Digicert for example can issue certificates for your domain.

One of the most wanted spammers gets arrested. Peter Levashov was arrested in

Barcelona while on vacation.

TP-Link 3G/Wi-Fi modem spews credentials. The M5350 3G/Wi-Fi router has an XSS vulnerability triggered by an SMS message containing the attack script. The device replies with admin username, admin password, SSID and its login password.

Hack sets off all of the emergency sirens in Dallas. 156 emergency sirens were set off for about an hour and a half.

15 ransomware decryption tools available for free. The important thing to remember here is that there is no guarantee these tools will work and the best thing to do is avoid being infected by Ransomware.

The difference in the various SSL certificates. You have probably heard the stories about Let's Encrypt issuing thousands of certificates containing the word "PayPal" and Google fighting with Symantec over their process for issuing certificates. Write-up has a nice explanation about the different types of certificates that are issued these days.

Shadow Brokers released the password for the cache of NSA's files.

Hackers can hi-jack the Aga oven with an SMS message. Apparently the oven has a phone number and the messages sent to it are completely unauthenticated.

Tech

Qualcomm countersues Apple over patent licenses. Qualcomm called Apple's lawsuit "baseless" and failing to engage in good faith negotiations for a license to its 3G and 4G patents. Basically they say Apple could not have built the iPhone without utilizing Qualcomm technology.

Parts of the federal government and financial sector are looking for COBOL experts. The Common Business Oriented Language was developed almost 60 years ago. Apparently it's estimated that $3 trillion in daily commerce flow through COBOL systems.

US Naval research testing swarms of palm-sized drones. The drones named CICADA (Close-In Covert Autonomous Disposable Aircraft) have sensors for measuring pressure, temperature and humidity and weighs only 65 grams. They are designed to be dropped from a tube on a Navy P-3 Orion aircraft. And they can land within a 5 meter square.

Detroit is beating Silicon Valley in the race to build self-driving cars. Navigant Research scored 18 companies engaged in self-driving technology and apparently GM and Ford are currently leading. Daimler and Renault-Nissan are close behind. It doesn't seem far fetched since these automakers are all well-versed in mass producing vehicles, more so than Tesla.

FCC plans to rollback net neutrality rules. Basically the FCC wants to reclassify broadband providers so that they are no longer subject to FCC oversight. ISPs appear to be getting carte blanche to do what they want with data on their networks whether its selling your data or shaping network traffic as they see fit.

Specs for Apple's new iMac. Details were leaked stating 64GB of memory and Thunderbolt 3. I really hope that memory limit carries over to the MacBook Pro soon.

J.D. Power tablet satisfaction survey shows Microsoft Surface beating iPad.

Tennessee mucks up fast internet deployment. They passed a bill called the Broadband Accessibility Act of 2017 which gives private telecom companies such as AT&T and Comcast $45 million of taxpayer money to build internet infrastucture to rural areas. The existing government owned company, EPB, which has already deployed 100Mbps, 1Gbps and 10Gbps connections and is profitable could have done it without taxpayer money. And the service provided by the telecoms will be 1000 times slower than what EPB could provide. Frankly that kind of law writing by telecoms is disgusting.

Random

Formula 1 racing in Bahrain this coming weekend

Drone sales doubled in 2016

FCC is doing something good for a change... kills plan to allow mobile phone calls on planes

Pew study finds that 70% of respondents believe government should be able to start their own high-speed networks

Apple drops to fifth place in laptop brand survey by Laptop Mag

Nintendo discontinues the NES Classic this month

Prison inmates stashed two hand built computers in the ceiling and used them to commit more crimes

Burger King creates an ad that intentionally activates the Google Assistant. That's going to be seriously annoying for Google and Amazon since they will now have to spend resources ignoring this kind of misuse of digital assistants.

Contact: @craigz28 on twitter or podcast@iotthisweek.com

If you don't have time to listen to the podcast, subscribe to the new IoT This Week Newsletter for weekly updates on interesting stories from the IoT, InfoSec and Tech world.

Contact: @craigz28 on twitter or email: podcast@iotthisweek.com