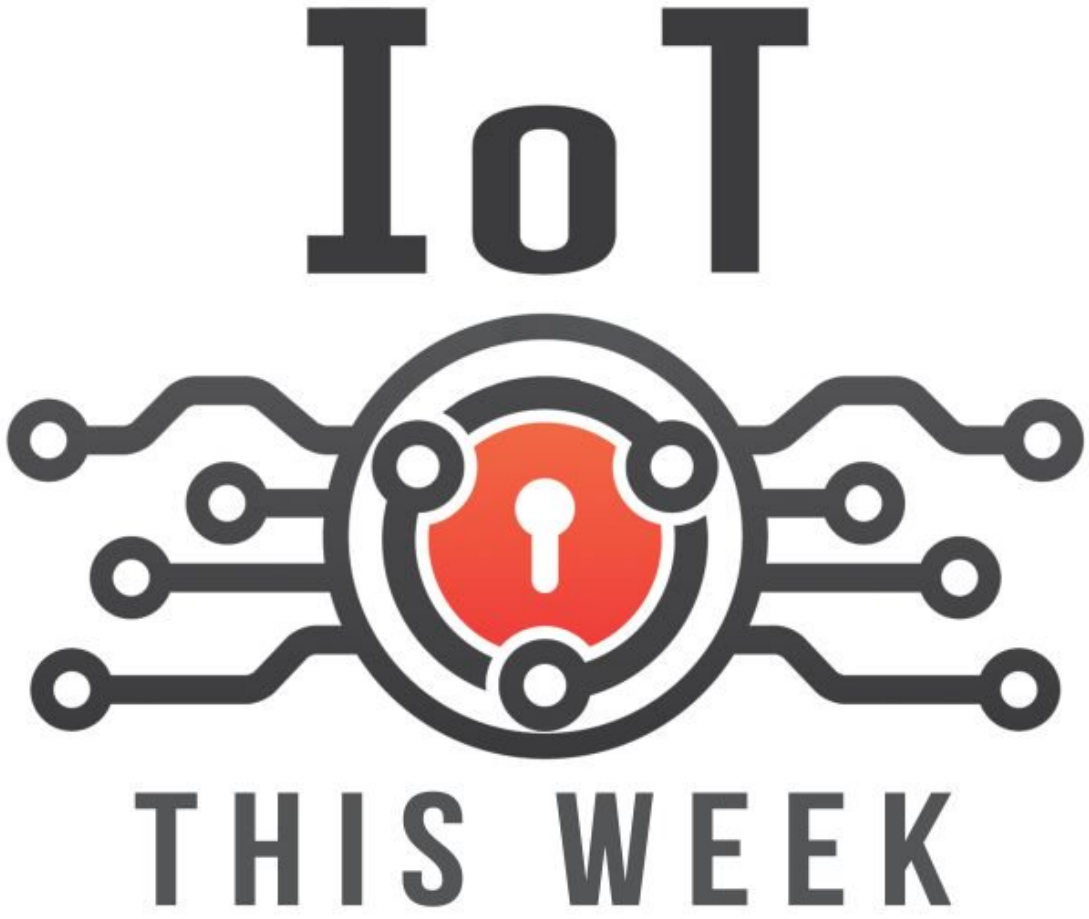

Episode 25

April 23, 2017

Catching you up on the latest from IoT, InfoSec and Tech. Episode 25 includes: IoT bot nets get crazier, fast and furious car hacking, IoT devices no one asked for, more data breaches, Uber's spiral continues and much more...

IoT

Cities are using IoT to map air quality by adding; 1) Adding sensors to existing infrastructure, 2) Mobile sensors, 3) Pairing sensors with mobile phone data. Chicago deployed sensors on lampposts to track the presence of carbon monoxide, nitrogen dioxide, ozone and particulate matter. Dublin put sensors on a bike share program to monitor some of the same things that Chicago did. And New York City used anonymized mobile phone data and combined that with air quality data to better understand exposure to people in areas of poor air quality.

Some things to address in IoT Security; Passwords, old software, if you don't need, don't keep it, giving away too much info, XSS, physical access attacks, use tested security measures,

Attempted code execution on Mirai honeypot after 59 seconds. The experiment was part of the McAfee Labs Threat Report: April 2017.

IoT malware called Hajime is spreading and creating a botnet with estimates of 100,000 infections so far. The malware doesn't use traditional command and control but instead uses peer-to-peer BitTorrent protocols which is harder to stop. Hajime also targets devices with ARM chips.

Interesting story from Dan Demeter's IoT honeypot. One of the things the researcher mentioned were the countries that were most probed; China and South Korea followed by the US and Japan.

Four critical steps to ensure IoT success; 1) Cut through complexity, 2) Make your data useful, 3) Architect for your analysis, 4) Secure opportunities.

How the car hacking in Fate of the Furious was filmed.

More flaws in Linksys routers found by IOActive. Cool thing here is that Linksys actually worked with the security company to fix the issues.

Seven RPi projects where you can make your own IoT device at home.

Flat transistors can provide every object with IoT capabilities. Using nanomaterials, they could be embedded in clothing, newspapers or cartons of milk.

WiLAN, a company that typically licenses wireless technology patents, is acquiring companies in the connected machines market.

OBD-II dongles can be attacked via Bluetooth. Researchers were able to hack Bosch's Drivelog dongle and inject malicious packets in the CAN bus.

15 idiotic IoT devices.

InfoSec

SparkCognition says AI is 99% effective for detecting malware. There is a beta program if you can make it in.

1000s of Windows hosts hacked using leaked NSA hack tools and show signs of DOUBLEPULSAR installed on them. Secure your Windows hosts.

Using corporate webmail for command and control and data exfiltration. When the typical avenues like web and DNS don't work.

Rapid7 finds a "low, consistent hum" from APT attack activity. Information from their April threat intelligence report.

Bose accused of tracking customer listening habits. They are collecting information via the app and then selling that information to marketers.

MasterCard adds fingerprint sensors to payment cards. Seems like more bad than good

from a broken system.

30,000 London gun owners hit by police "data breach". The "data breach" was actually the police selling the information to marketers.

InterContinental hotel chain data beach expands. Affects many of their brands so check your credit card statements if you've visited lately.

$175 ransomware service available on the internets. SAAS for ransomware I suppose.

Punycode phishing attacks using known browser vulnerabilities. This has mostly been been fixed except for Firefox I believe.

Survey finds breaches depress share price. I'm kind of surprised since I believe people mostly don't care about breaches any longer.

Tech

Apple wants to make the future iPhone from purely recycled materials. So no more mining new materials, only using recycled materials.

Apple Pay still feels like the future. I really wish plastic payment cards would go away.

Amazon opens up the voice control technology behind Alexa. They want to use it for further data collection to make the technology better.

Perceptual ad blocking puts advertisers on their heels. Basically a concept to try and look at ad blocking like a human and do it in the browser.

Company pay millions of dollars for white hat hacking. No surprise and is good for security overall.

Uber supposedly tracked users even after they deleted the app. They say they didn't. We'll see.

John Deere tells the copyright office that only corporations can own property and humans can only license it. More nonsense from John Deere and their war against their customers.

Apple forces recyclers to shred all iPhones and MacBooks. I guess this is good for their new initiative to only use recycled materials but prevents extending the life of used products.

Random

Formula 1 racing in Russia this coming weekend

The original StarCraft is now free

Some guy made a robot that targets eyeballs and fires a laser

Google Home can recognize more than one person now

Amazon Echo can now add events to your Google Calendar

Awesome Hacking project on Github

Verizon sees record subscriber losses to T-Mobile

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

---