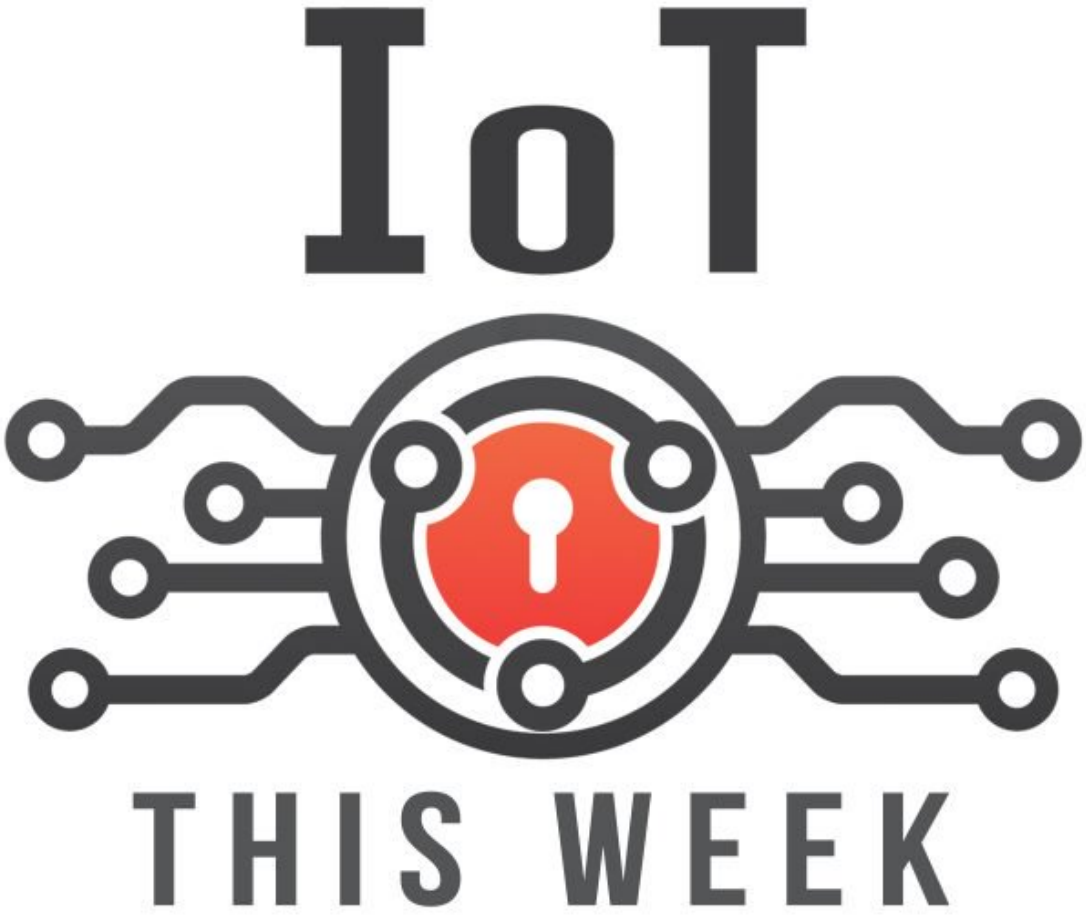

Episode 26

May 1, 2017

Catching you up on the latest from IoT, InfoSec and Tech. Episode 26 includes: Smart diapers, vulnerable cable modems, IoT botnets, the Internet of Cows, threat intelligence reports and much more...

IoT

Monit, a Korean company has a new Bluetooth sensor which can alert parents when a diaper is soiled. In the future, the sensor will be able to determine air quality and temperature.

Intel powered broadband modems vulnerable to DoS attack. Puma 6 Intel cable modems are susceptible to low bandwidth DoS attack. Puma 6 modems are sold as gigabit broadband gateways and is used by a number of ISPs including Comcast and Virgin Media.

Hundreds of thousands of cable modems around the world are vulnerable due to a weakness in the Simple Network Management Protocol (SNMP). Researchers found a way to bypass SNMP authentication on 78 models of modems. The vulnerability has been dubbed StringBleed.

Check Point wants to design in- car data protection since it already provides secure

communication between cars and the cloud.

Hajime botnet continues to infect vulnerable IoT devices and block access to four ports known to be used as attack vectors. It also displays a signed message describing its maker as "just a whitehat, securing some systems."

Cloudflare Orbit is a private network for IoT devices.

Brickerbot has killed over 2 million insecure IoT devices.

The Internet of Cows hackathon hosted by BovControl, a Brazilian startup building data analytics to support livestock operations.

Hyundai Blue Link vulnerability allows remote start of cars.

WISeKeyIoT framework offers digital Public Key Infrastructure (PKI) certificates for connected devices.

InfoSec

Kali Linux can now use Cloud GPUs for password cracking. The new version 2017.1 supports GPU instances in Azure and AWS and also adds support for RTL8812AU wireless chipsets.

Hundred of applications on Google Play Store open ports on smartphones exposing millions of mobile devices to potential attacks.

Russian controlled telecom hijacks traffic for Mastercard, Visa and other services.

Fileless malware attacks continue. This type of malware is exactly how it sounds, instead of dropping files, it stores information in system memory.

CIA tool to track whistleblowers and spies leaked on Wikileaks.

Futurepets.com exposes details of more than 110,000 credit cards.

Chipolte notifies customers of a potential payment processing breach between March 24th and April 18th.

New MacOS malware is signed with legit Apple ID and spies on HTTPS traffic.

New OWASP Top 10 published.

Fundamentals of fingerprint scanning gives an overview of three common ways to scan a fingerprint.

Tech

Apple may be launching a peer-to-peer payment service for Apple Pay.

FCC planning to reverse net neutrality at meeting on May 18th.

US Court of Appeals for the DC circuit denied an ISP request to overturn a previous ruling on net neutrality rules.

Tech IPOs are coming fast this year. Nine companies have gone public this year as opposed to one by this time last year.

Random

Comcast likely not serious about entering wireless market fray

In 1973, three crew members of the NASA Skylab mission went on strike for 24 hours.

One-third of federal agencies reported data breaches in 2016

Iowa farm cartoonist fired after creating a cartoon that mentioned Monsanto, DuPont Pioneer and John Deere

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

---