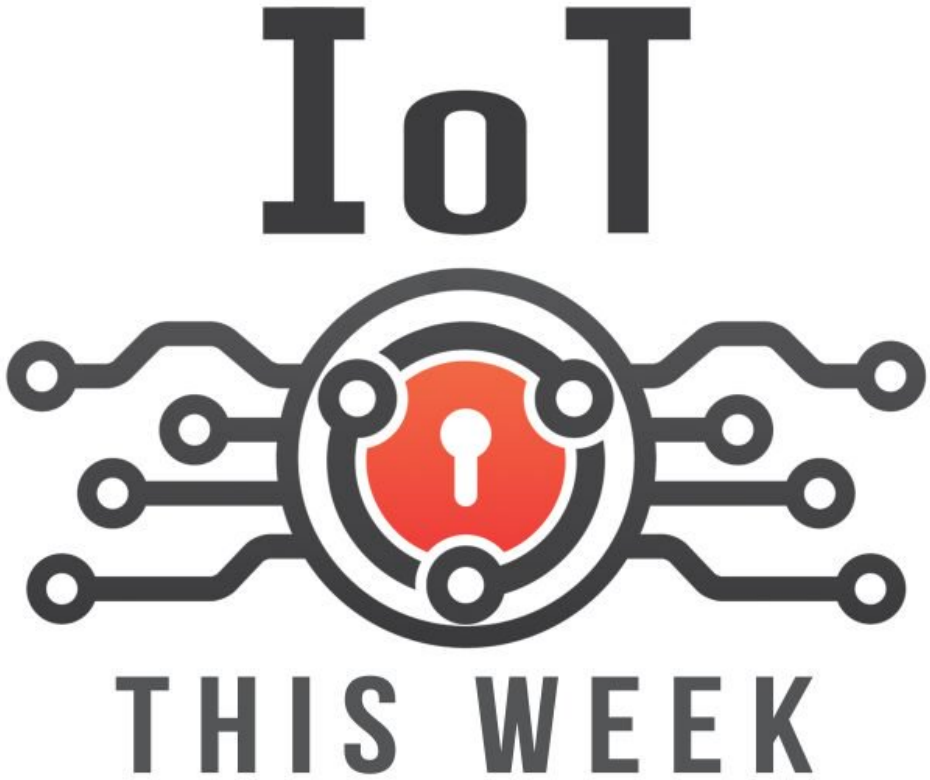

May 29, 2017

Catch up on the latest from IoT, InfoSec and Tech. Issue 30 includes: Pacemakers riddled with vulns, Galaxy S8 iris scanner broken, smart lock maker forced to do security, RDP exploits, Android malware, the dead comment on net neutrality, Doom on a thermostat and much more...

IoT

Radio controlled pacemakers are vulnerable to attack according to a report from WhiteScope. Among the findings was extensive use of third-party libraries, hardcoded credentials, unvalidated firmware, removable media, unencrypted on-device patient data, etc. A pattern of findings we have seen in many other IoT devices.

A study by Cisco shows that 60% of IoT projects stall at the Proof of Concept phase and only 26% of companies have an IoT project they consider to be a complete success.

A US senator sends a letter to the FTC asking it about efforts to protect the privacy of kids when they use toys like CloudPets. Germany banned CloudPets over privacy concerns.

New York state forces a smart lock maker, Safetech, to improve its security by

adding encryption to protect passwords, electronic keys and other credentials on the locks and prompt users to change the default password upon initial setup.

The Cloud Security Alliance released a research report on connected vehicle security. Risks include vehicles communicating with both legacy and modern traffic infrastructure, the interaction of traffic management applications with cloud services, the installation of OEM and 3rd party applications and traffic infrastructure and the integration with IoT systems to support vehicle communication with smart homes.

InfoSec

Judy Android malware is infecting over 36.5 million Google Play store users according to Checkpoint. The apps created by Kiniwini create fake advertisement clicks from the infected devices.

SSDs may be vulnerable to an attack similar to the Rowhammer attack on RAM memory chips.

Chipolte says most of its restaurants were infected with credit card stealing malware. The vulnerable time frame was between March 24th and April 18th, 2017. They have also released a tool to help customers check if a restaurant they visited was involved.

The FTC states that it takes criminals only nine minutes to use stolen consumer information. They determined this by posting fake but realistic consumer data on a site used to make stolen data public.

The master keys associated with the Crysis ransomware have been released to the public.

Researchers find that 82% of databases are not encrypted in the public cloud while 31% were accepting incoming connections from the internet. 51% of network traffic in on the default port of 80 and 93% of public cloud resources have no outbound firewall rule.

NIST started a lightweight cryptography project back in 2013 and has now come out with their first report. The project is targeted at embedded systems, RFID devices and sensor networks.

The EsteemAudit RDP exploit remains unpatched on no longer supported Windows Server 2003 and Windows XP hosts.

A new type of attack vector dubbed "Cloak and dagger" is affecting Android devices. The attack allows a malicious app to completely control the UI feedback loop and take over the device.

Scammers are pushing anti-WannaCry Android apps even though the ransomware only targets Windows.

The Chaos Computer Club breaks the iris recognition system of the Samsung Galaxy S8 by using a camera, a printer and a contact lens.

The massive 2013 Target breach costs them $18.5 million in a settlement made with 47 states and the District of Columbia. 70 million customers were affected by the breach.

Tech

A Tesla owner is gleaning information from Tesla's Autopilot by placing the system in debug mode.

Researchers say they have found the exact mechanism which allowed diesel Volkswagons and Audis to cheat emissions testing. In 2015, regulators realized these vehicles were emitting several times the legal limit of nitrogen oxides.

Deceased individuals have been posting anti-net neutrality comments to the FCC website. At least 500,000 comments appear to have been posted by bots.

MIT engineers have designed a workout suit that responds to body heat and opens/closes vents accordingly.

An enterprising person got the game Doom to run on a Honeywell thermostat.

Miscellaneous

Comcast tried to censor a site that claimed it was committing fraud. They eventually backed down from their threats.

After two independent security audits earlier this month, a security company went public with a vulnerability discovered in the admin interface for OpenVPN's server. The vulnerability was something not discovered during the audit.

If you ever wondered about Android encryption, this article will help shed some light on it.

A Texas bill could mean jail time if you fly a drone over oil facilities.

A study by Fluent states that more than half of streaming users share their passwords.

Listen to the latest IoT This Week podcast.

Subscribe to the new IoT This Week Newsletter for weekly updates on interesting stories from the IoT, InfoSec and Tech world.

Follow @iotthisweek on twitter for the latest tweets on interesting stories.

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

---