


# IoT

The logo features the text 'IoT' at the top in a large, bold, black sans-serif font. Below it is a central graphic consisting of a red shield with a white keyhole in the center, surrounded by a black circular border. From this central circle, several black lines radiate outwards, each ending in a small white circle, resembling a circuit board or a network diagram. At the bottom, the text 'THIS WEEK' is written in a bold, black, sans-serif font, spaced out.

## THIS WEEK

May 7, 2017

Catching you up on the latest from IoT, InfoSec and Tech. Issue 27 includes: Hacking industrial robots, Intel's AMT is a mess, US DOJ investigates Uber, servers mining cryptocurrency and much more...

## IoT

[Researchers](#) found 80,000 industrial robots exposed to the internet. Trend Micro detailed a PoC attack against a ABB Robotics IRB140 industrial robot exploiting a remote code vulnerability in the controller software. The robot was given a modified configuration file changed its parameters for drawing a straight line.

[New update](#) capabilities were revealed by the company Everynet. It's for IoT devices on LPWA networks and will allow manufacturers, operators and users to more easily update those devices. The new patent pending technology forces the compiler to come with the minimum difference between the old firmware version and the new one. That difference along with a new compression algorithm is the only thing sent to the device for updating purposes.

[Microsoft](#) has a new approach to securing IoT called Project Soprois. The project looks to deliver both secure hardware and a secure communication channel. They essentially want to bring many of the trusted computing models used in Windows to IoT devices. Microsoft also issued hardware to about 150 security folks with specific bug bounties in place.

There's a new [IoT processor](#) called GAP8 put out by Greenwave Technologies. The processor is meant to be extremely power efficient for use in battery powered data-rich sensors analytics and software defined radio.

[Amazon and Conexant](#) created a development kit for third-party manufacturers looking to build Alexa in their devices.

[Interesting](#) story on [hackaday.io](#) where a person wanted to install a reversing camera in his old Peugeot 207 and ended up reverse engineering the CAN bus.

[Disney Research](#) has devised an ultra-low power system of sensors that transmit data to a central receiver by reflecting the ambient radio waves from commercial broadcasting systems that already cover most office environments.

## Security

The [Mac version](#) of the popular video transcoder HandBrake was apparently hacked and a malicious version made available between May 2nd and May 6th. If you downloaded and installed HandBrake between those dates, do check out HandBrake's web site for instructions.

The issues with [Intel's AMT](#) toolkit continue with attackers able to access the login page by simply sending an empty login string. There are currently thousands of host on the internet exposing the login page via port 16992 and 16993.

[Intel](#) releasing a patch this week to fix the issues with AMT.

The [average ransomware](#) demand is now over \$1000 according to Symantec. Other estimates put total ransomware revenues at over \$1 billion dollars last year. 34% of people paid the ransom globally, but in the US, the percentage of people paying the ransom is 64%.

There's a [Wordpress flaw](#) that could allow attackers to reset the admin password. The flaw affects all versions of Wordpress. The vulnerability involves the password reset email and has been reported to Wordpress on multiple occasions starting back in July 2016.

[Europe](#) spews out 50% more cybercrime attacks than the US according to ThreatMetrix Q1 Cybercrime Report. Most of the attacks from Europe came from the UK and Germany.

[Shodan](#) released a new tool called Malware Hunter. It's a tool for identifying devices on the internet that are serving as command and control (C2) for remote access trojans (RATS)

The [company](#) that Shodan partnered with to develop this new tool, Recorded Future, also has an interesting threat intelligence report out as well.

A [Google Docs](#) phishing scheme is spreading rapidly so if you receive any emails stating that a person has shared a document on Google Docs with you, don't click it and delete the

email immediately.

A [Florida](#) state court has ruled that two people facing extortion charges do not have constitutional protection against being forced to hand over their phone unlock codes.

[135 million](#) Indian government payment card details were leaked. The breach wasn't against the Aadhaar project itself but attributed to government agencies leaking Aadhaar and related data they had collected for their own purposes.

## Tech

[Citigroup](#) analyst listed seven companies as potential takeover targets for Apple; Netflix, Disney and Tesla among the them. Apple currently has cash of more than \$250 billion.

[Apple](#) named world's largest wearable vendor. They had an estimated 3.5 million Apple Watch shipments in Q1 2017. Apple overtook Fitbit in shipments during Q1 as well.

[Qualcomm and Apple](#) are in a patent war and Qualcomm is looking to block US imports for iPhones.

[UAE](#) is looking to start a project for dragging an iceberg from Antarctica to help solve a water shortage. An average iceberg contains more than 20 billion gallons of fresh water. The project is set to begin in 2018.

[US Department of Justice](#) is investigating Uber's "Greyball" program. The program helped them sidestep law enforcement officials and regulators.

[Square](#) is inviting users to sign up for its debit card. The debit card will only be linked to your Square Cash app.

## Miscellaneous

[Thousands](#) of hacked servers found to be mining cryptocurrencies.

[Snake malware](#) targeting Macs via fake Adobe Flash Player installer.

[Microsoft](#) testing a malware proof Edge browser.

Most [American](#) households have abandoned their landlines.

[Another tool](#) has been leaked from the Vault 7 series called Archimedes reportedly used to attack computers inside a LAN.

[Apple](#) revokes certificate of malware that used a legit Apple ID and spied on HTTPS traffic.

---



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.

Contact: [@craigz28](#) on twitter or email: [podcast@iotthisweek.com](mailto:podcast@iotthisweek.com)

---