IoT THIS WEEK

May 14, 2017

Catching you up on the latest from IoT, InfoSec and Tech. Issue 28 includes: More IoT botnets, WannaCry ransomware, HP key logging, don't hack you former employer and much more...

IoT

Another IoT botnet called Persirai is targeting more than a thousand internet protocol camera models. Trend Micro reported that 120,000 web-connected cameras are vulnerable to malware.

Multiple vulnerabilities in Asus routers including CSRF, JSONP and XML. Most were fixed in a March 2017 firmware update except the JSONP issue.

A map of 263 companies working towards autonomous cars. Most you've probably never heard of.

The Hackaday Prize 2017 is on hackaday.io. The Internet of Useful Things challenge two has begun.

More than half of UK drivers fear connected car hacking according to a study by the Institute of the Motor Industry.

Interesting article on what data breaches mean for IoT. One of the main points being that there is no single data breach notification standard at the US federal level. Standards are currently on at the state level.

Charlie Miller and Chris Valasek have released all their research including how they hacked a Jeep Cherokee and other vehicles.

InfoSec

SMB honeypot gets infected with WannaCry ransomware six times in 90 minutes.

According to MalwareTech the WannaCry ransomware has made over 223,000 victims, but has only made $31,000.

WannaCry is based on the EXTERNALBLUE exploit leaked online.

A researcher temporarily stopped the WannaCry ransomware by registering the domain name **iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com** which the malware would ping and if it wasn't registered the the encryption process would begin. Some people misunderstood this process and blocked the domain causing the ransomware to continue its spread. A new version without this kill switch is supposedly out in the wild now.

New strain of ransomware called Jaff is spreading via the Necurs botnet and asking for a ransom of 2 BTC which is about $3600 now. Jaff may be the same folks behind Locky, Dridex and Bart. It appears that only a couple victims have been identified at this point.

All OnePlus mobile phones are vulnerable to remote attacks due to four issues discovered by a security researcher. The vulnerabilities facilitate man-in-the-middle attacks allowing a remote attacker to replace the device's operating system.

Several HP laptop models silently recorded everything you typed on the keyboard via an HP audio driver. The log file is saved in the c:\Users\Public\MicTray.log.

A former security officer for the company Tyan Inc. was ordered to pay more than $300,000 for attacking his former company's computer systems.

True Health Group exposed logged in users to other user's data simply by changing a single digit in a link attached to a PDF for viewing a user's latest health report.

Microsoft released an emergency patch for a vulnerability discovered in its Malware Protection Engine. One researcher called it the worst Windows remote code execution vulnerability in quite a while.

A draft version of NIST's password guidelines was met with approval by vendors. The new framework recommends among other things; 1) removing periodic password change requirements, 2) dropping the algorithmic complexity requirement, 3) requiring screening of new passwords against list of commonly used or compromised passwords.

Tech

Apple Watch can detect an abnormal heart rhythm with 97% accuracy when paired with an AI-based algorithm. The study involved 6,158 participants recruited through the Cardiogram app.

A recent survey of 2,345 US millennial and Gen Z shoppers found that the Amazon app was the 2nd most popular app among those surveyed.

Cloudflare offers a $50,000 bounty to anyone who can help invalidate a patent claimed by a patent troll.

The rush is one for Ethereum domain names. Ethereum is block-chained based so getting a domain name will be a bit different than how we normally think of acquiring domain names on the web.

Apparently bots flooded the FCC website for net neutrality comments with fake anti-net neutrality comments. This tactic has been used by large ISPs in the past and the people who are used to post comments under typically have no idea it was done.

An article on everything you need to know about NFC.

Amazon enables free calls and messaging through Echo devices using the Alexa app. There are some issues with it like not being able to block calls, etc.

Apple nears $800 billion valuation on its way to becoming the first trillion dollar company.

Miscellaneous

Patents on MP3 format are close to expiring.

Mastercard aims to speed up chip-and-PIN payments.

Google launches Fuchsia OS.

You can pay your American Express bill with Amazon's Alexa now.

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