CommsWire
Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Wednesday 16 January 2019

HAPPY NEW YEAR – TIME TO CHANGE YOUR ISP

CommsWire (ISSN 2202-4549) is published by iTWire Pty Ltd. 18 Lansdown St, Hampton, Vic, 3188
CommsWire/Telecommunications Editor: Stan Beer
Staff writers: Peter Dinham, Alex Zaharov-Reutt, Sam Varghese. Columnist: John de Ridder
Advertising: CEO and Editor in Chief, Andrew Matler: andrew.matler@itwire.com • Tel: 0412 390 000

MANY AUSTRALIANS TO CHANGE INTERNET PLANS AFTER XMAS

Product comparison firm iSelect says it has seen an average increase of 40% in the number of Australians inquiring about changing Internet plans after the festive season.

A survey conducted by YouGov Galaxy for iSelect found that more than half (51%) of the 1000 Australians whose opinions were canvassed indicated that the bandwidth they consumed increased during summer.

iSelect spokesperson Laura Crowden said the survey indicated that the number of connected devices exchanged over Christmas was one factor that many families to reconsider their current Internet plans.

“For the past four years, iSelect has seen an average 40% increase in the number of customers enquiring about a new Internet plan in early January,” she said.

“This is driven by a combination of new connected devices for Christmas, higher Internet usage due to the whole family being at home and many of us finally having the down-time to review our current plan.”

The survey, carried out before Christmas, also found that at least 30% of the participants were expecting to either give or receive a connected device as a gift for the festival.

Crowden said the average Australian home now had more than 17 connected devices, compared to 14 in 2018, and this was expected to rise to 37 by 2022.

“Many of us were lucky enough to unwrap new connected devices at Christmas and with parents off work and kids on school holidays during January, more time is spent online, streaming entertainment, playing video games or simply browsing the web," she said.

“Time off in January also means a bit more spare time for many parents to finally get around to those life admin tasks that have lurked on their to-do list for the past year and it seems reviewing their internet plan is high on the list for many households.”

Crowden said choosing the right Internet package could be confusing, given the overwhelming number of plans and providers all competing for new customers.

Sam Varghese

MOTOROLA PAYS US$445M TO BUY DATA ANALYTICS FIRM

Global communications heavyweight Motorola Solutions has paid US$445 million to acquire VaaS International Holdings, a data and image analytics company based in Livermore, California and Fort Worth, Texas.

VaaS, which describes itself as a company that does "video analysis as a service", is a global provider of data and image analytics for vehicle location and image capture.

Its analysis platform, which includes fixed and mobile license plate reader cameras driven by machine learning and artificial intelligence, provides vehicle location data to public safety and commercial customers.

Its subsidiaries include Vigilant Solutions for law enforcement users and Digital Recognition Network (DRN) for commercial customers.

VaaS claims 2019 revenues which are expected to be approximately US$100 million.

The company's research and development operations are based in Vietnam where it has more than 40 employees working in software engineering, AI and data analytics.

"This acquisition expands Motorola Solutions' data and analytics capabilities, complementing our public safety software and analytics suite and Avigilon video and analytics platform," said Greg Brown, chairman and chief executive, Motorola Solutions.

"VaaS will enhance Motorola Solutions' software portfolio with vehicle location information that can help first responders shorten response times, improve the speed and accuracy of investigations and create safer cities."

"We are very excited to be joining Motorola Solutions," said Shawn Smith, co-founder of VaaS and president of Vigilant Solutions.

"This acquisition enables us to continue to serve our existing customers and expand our footprint globally, while at the same time supporting a company with a commitment to innovation and growth, guided by a common purpose that aligns with our mission and culture: 'To help people be their best in the moments that matter.'

"It doesn't get any better than that."

"Our extensive license plate data and AI technology have opened new commercial applications of our products," said Todd Hodnett, co-founder of VaaS and president of Digital Recognition Network.

"We believe commercialisation of these new applications can be accelerated under the Motorola Solutions brand and reach, and we look forward to working together to grow and diversify our commercial business."

Peter Dinham

HUAWEI FOUNDER CLAIMS NO USER DATA WILL BE GIVEN TO GOVT

Huawei chief executive and founder Ren Zhengfei says the company will under no circumstances allow the Chinese Government to access customer data.

During a media conference in Shenzhen on Tuesday, Ren sought to address concerns raised by the US that has repeatedly claimed the Chinese telecommunications equipment giant could allow the government a backdoor into a country's communication systems.

CNBC **quoted** Ren as saying: “When it comes to cyber security and privacy protection we are committed to be sided with our customers.

“We will never harm any nation or any individual.

“China’s ministry of foreign affairs has officially clarified that no law in China requires any company to install mandatory backdoors.

“Huawei and me personally have never received any request from any government to provide improper information.”

The US has banned the use of Huawei equipment in its 5G networks, claiming that the company can be a conduit for spying by Beijing.

Australia and **New Zealand** have both followed the US lead and banned the company from roles in their respective 5G rollouts.

Apart from the pressure on the company over 5G, its chief financial officer Meng Wanzhou, Ren's daughter, was **arrested** in Canada last month following on a request from the US, which claims she has been involved in breaking American sanctions on shipping US-made equipment to Iran.

Ren did not offer any comment about the arrest of his daughter.

He foresaw a difficult year ahead for the company, with revenue growth falling below 20%, adding that it was targeting US$125 billion for the year.

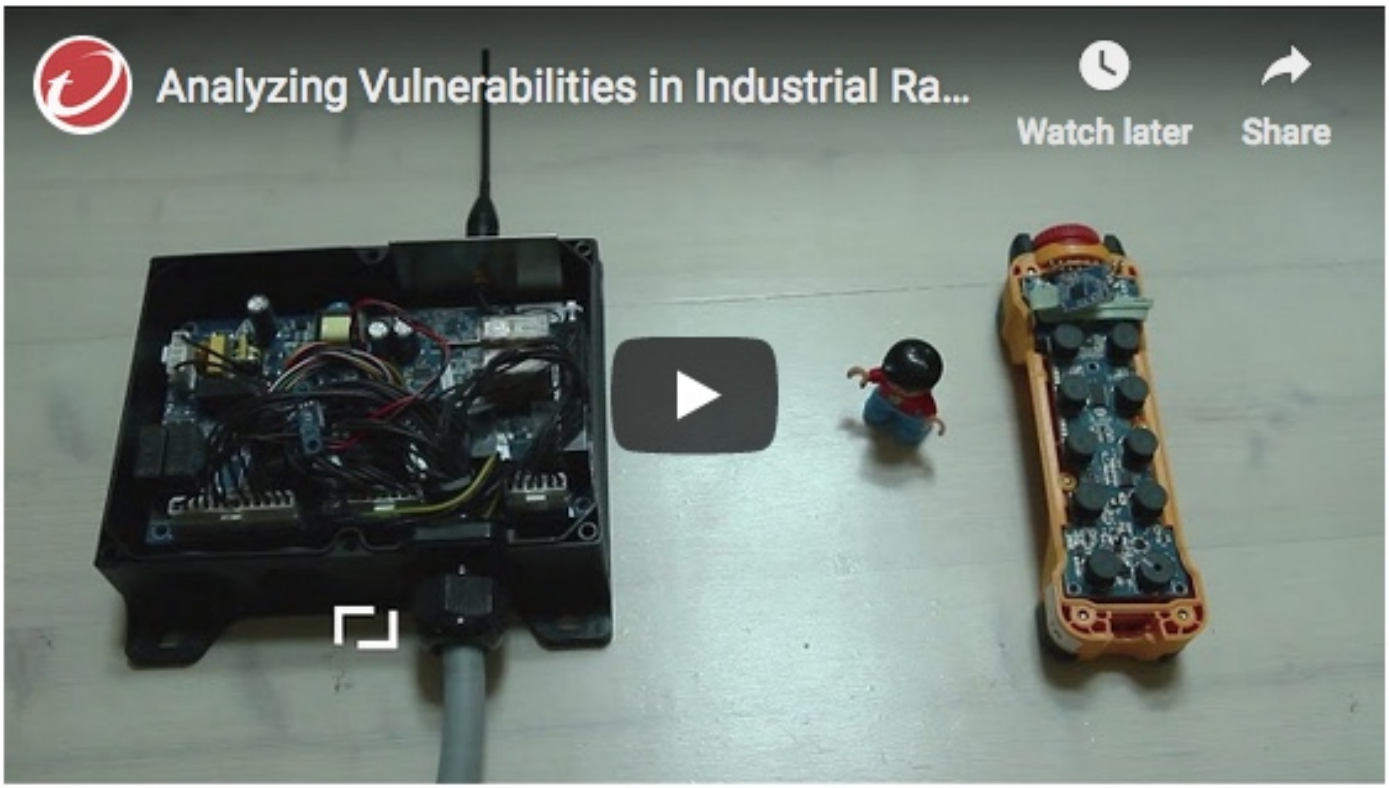
“In 2019 we might face challenges and difficulties in international markets. That is why I said ... our growth next year would be less than 20%," he added.

Sam Varghese

FIRM DEMONSTRATES HACK OF RF-CONTROLLED MACHINES

Researchers at security outfit Trend Micro have built a device they call RFQuack, which can be used to hack into and take command of industrial machines that are controlled through radio frequency protocols.

A blog post by the company said RF protocols were often used to control simple operations of industrial machines, like switching on a motor, lifting a load or manoeuvring a heavy vehicle.



The Trend Micro team said it had been able to perform attacks from within or from outside the RF range.

Remote attackers from outside the RF range could either carry out a computer-borne attack — or take control of a computer used to either program or control the RF device — or obtain temporary access to the facility where the device was located and leave behind an embedded device for remote access.

The device that the researchers built, known as RFQuack, was used as a tool for studying the attacks that could be carried out.

RFQuack can be controlled remotely through Message Queuing Telemetry Transport messages sent from a client-side interactive console that the researchers built around it.

The device also works under Wi-Fi, 3G, and 4G conditions.

"When powered up, the device stays idle to save power. When set to receiving mode, it goes into deep-sleep mode and wakes up only when a valid radio packet is received," the researchers said.

"When a valid packet is received, its default behaviour is to resend it immediately enough times to make the target receiver 'obey' the command.

"In fact, before retransmission, RFQuack has modified the packet on the fly, according to a configurable set of rules.

Alternatively, RFQuack can be used to collect radio packets or just send manually crafted packets."

Controllers could be attacked and used to control construction cranes. industrial cranes and mobile hoists in production settings, the team said.

Such industrial devices tended to be used for a long time in production; given that support times would expire, it would be impossible to obtain patches as new products would have replaced the old ones.

Trend Micro suggested the following measures to minimise the risk of this type of attacks:

- Inspecting technical manuals before purchasing a device (most of the manuals are available even online) and ensuring that some form of configurable pairing is available;
- Periodically changing the fixed (ID) code, if possible;
- Keeping the programming computer off the network or hardening its security as if it were a critical endpoint;
- Preferring remote control systems that offer dual-technology devices, such as those with virtual fencing; and
- Choosing devices that use open, well-known, and standard protocols such as Bluetooth Low Energy.

Businesses were advised to ensure secure protocols and processes by:

- Implementing rolling-code mechanisms (or better) and providing firmware upgrades to devices;
- Building on open, well-known, and standard protocols like Bluetooth Low Energy (which some vendors are already doing);
- Considering future evolutions when designing next-generation systems; and
- Using tamper-proof mechanisms to hinder reverse engineering (most of the products that we've analysed are easily accessible.

Sam Varghese

GERMAN COURT DISMISSES QUALCOMM SUIT AGAINST APPLE

A court in Germany has dismissed a patent lawsuit filed by processor maker Qualcomm against Apple, saying that the patent concerned was not violated by its chips in iPhones.

Tuesday's verdict is over a patent that concerns bulk tension of voltage in iPhones, and the court ruled that Apple did not violate Qualcomm's patent because smartphones do not have steady voltage.

Last month, a court in Munich ruled in favour of Qualcomm in another patent case, which was over IP for power savings in smartphones.

Apple was ordered to stop selling some older iPhone models at its stores in Germany as a result.

But all models are available at third-party stores in the country. Apple has appealed this verdict.

Qualcomm said it would appeal against Tuesday's verdict.

The company's executive vice-president and general counsel, Don Rosenberg, said: “Apple has a history of infringing our patents.

"Only last month the Munich Regional Court affirmed the value of another of Qualcomm’s cutting-edge patents against Apple’s infringement and ordered a ban on the import and sale of impacted iPhones in Germany.

"That decision followed a court-ordered ban on patent-infringing iPhones in China as well as recognition by an ITC judge that Apple is infringing Qualcomm’s IP.

"The Mannheim court interpreted one aspect of our patent very narrowly, saying that because a voltage inside a part of an iPhone wasn’t constant the patent wasn’t infringed. We strongly disagree and will appeal.”

In December, Qualcomm **obtained** a court order in China imposing a ban on the import and sale of some iPhone models. Apple has appealed that decision as well.

Sam Varghese