CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Tuesday 18 June 2019

US BANS TO COST HUAWEI $25B SAYS FOUNDER

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

HUAWEI FOUNDER SAYS US BANS WILL COST COMPANY US$25B

Chinese telecommunications equipment provider Huawei Technologies says it will suffer a drop of US$25 billion in projected revenue over the next two years, compared to its earlier forecasts, due to the American Government's actions against it.

The company's chief executive and founder, Ren Zhengfei, told a panel discussion in Shenzhen on Monday that it expected revenue to fall to US$100 billion in 2019, compared to US$105 billion in 2018. In Februiary, a target of US$125 billion had been set for the 2020 financial year.

Ren made the statement during a panel discussion at Huawei headquarters along with futurist, author and venture capitalist George Gilder, MIT Media Lab co-founder Nicholas Negroponte and Huawei senior vice-president and board member Catherine Chen.

The discussion was moderated by Tian Wei, host of China Global Television Network's World Insight.

"We never thought the US would attack us on such a broad front," Ren said. "But this can't stop us from proogressing. We didn't expect it to be so serious.

"We made some preparations, but it was like a broken airplane with only the heart, the fuel tanks. We didn't protect the other necessary parts.."

He said Huawei would lose about 40% of its smartphone sales overseas due to the punitive action taken by Washington.

The US Government placed Huawei and 68 of its affiliates on its Entity List on 16 May, meaning that the company would have to seek permission to purchase any American components it needed to manufacture its products.

Four days later, Google announced it was cutting off Huawei's access to future updates of Google's Android and Google Play Store.

Huawei, which is now the second biggest smartphone vendor globally after Samsung, uses a customised version of Android on all its smartphones and tablets.

On 21 May, the US Commerce Department eased some of the restrictions until August, allowing Huawei to maintain and update existing networks and handsets.

Sam Varghese

NBN CVC PRICE MAY FORCE LAUNTEL TO STOP 250/100 ACT PLANS

Tasmanian-based Internet services provider Launtel says it is likely to stop offering its 250/100Mbps NBN service in Canberra due to the "extremely expensive" CVC charges imposed by national broadband network provider NBN Co.

In a blog post, Launtel chief executive Damian Ivereigh said NBN Co's CVC pricing construct was the factor that had led to the company reconsidering its offering of this service.

"It is extremely expensive to offer these services for a relatively small number of people and we are very disappointed to say that it looks like we will just have to stop offering it," he added.

Ivereigh (left) pointed out that to support 250/100 services, he had to buy about 750Mbps of CVC, an extra 450Mbps above what the NBN Co offered free to get past the scaling issues.

This meant an extra $3600 each month over what was needed for the 100/40Mbps service.

"We don’t actually buy that much, [we buy] about 600Mbps and unfortunately we are seeing some occasional congestion when two people on 250Mbps service fire up at the same time, during peak times," he explained.

"We don’t have many 250/100 services – around 15 – so that’s $240/month per connection, around $8/day.

“This is just the CVC! Add in the AVC charge and it’s about $11/day just for the NBN component. So, yes, we are making a big loss on 250/100 services!"

ISPs have to pay two kinds of charges to NBN Co. The AVC is a single price per connection based on the peak speed of that connection which means that higher speeds would cost more.

The second charge is for CVC – the total bandwidth that an ISP requests to use across all its services in an area. It is called a CSA which is just a point of interconnect.

"In Canberra there are two CSAs: Civic and Queanbeyan," Ivereigh said.

"If an RSP does not purchase enough CVC then the result is congestion at peak times as there isn’t enough bandwidth to go around.

“NBN Co and the RSPs assume that a certain amount of CVC, typically just a few Mbps, is used on average per connection.

“So for example if 2.5Mbps of CVC is allocated per connection, then if you have 1000 services, then your CVC should be 2500Mbps."

Ivereigh said the issue with this calculation was that it did not scale down.

"You have to have a minimum amount of CVC just to allow a service to work at all. Clearly, you have to have at least 100Mbps of CVC just to allow a single connection to peak at 100Mbps.

“However when you have two, you probably need 200Mbps so they can both operate at the same time.

“However when you get more, you can start going back to the old formula. The received wisdom is that you need about three times the highest speed of your services as a minimum on your CVC."

Ivereigh said NBN Co had recognised this scaling issue and allowed an RSP to get a minimum of 300Mbps of CVC effectively free to get past this, a gesture that was clearly aimed at supporting 100Mbps services.

"Great what about higher speed ones? Unfortunately, NBN Co has done nothing to help.

“If RSPs want to sell 250Mbps and above, they need to buy more CVC, at $8/Mbps/month," he said.

"The problem is that all that extra CVC is really just to support the higher speed services and it gets really expensive per service."

He said Launtel was able to keep offering the 250/100 service in Tasmania because it had gone past the scale issue.

"We have about 10 times the number of connections in Tasmania that we have in Canberra, plus we set up our gigabit network in Tasmania mainly for businesses, whose CVC capacity we can use at night!"

Regarding the NSW connections, Ivereigh said the problem was that as the price got higher, less people wanted to buy it.

"But the CVC cost is the same, just spread over fewer people, making our cost per service higher. A vicious cycle," he added.

"To make matters worse our daily pricing works against us – people, quite reasonably, will just upgrade for the day just for some big downloads. The problem is we have to keep (i.e. buy) the bandwidth on hand regardless."

Sam Varghese

ERICSSON LAUNCHES ENHANCED 5G DEPLOYMENT OPTIONS

Swedish telecommunications infrastructure provider Ericsson has launched new software and hardware solutions to expand 5G deployment options, with the new solutions claimed to be extending network capacity and coverage.

Announcing the expansion, Ericsson said the new solutions enabled smooth network evolution, and facilitated new consumer and industry use cases.

While already supporting frontrunner service providers through the rollout of commercial 5G using non-standalone 5G New Radio, Ericsson has now introduced standalone NR software.

Ericsson says that, in addition to extending deployment possibilities, 5G standalone NR software makes for, “a new network architecture, delivering key benefits such as ultra-low latency and even better coverage.”

The company says it is also evolving its cloud solution with an offering optimised for edge computing to meet user demand, which will enable service providers to offer new consumer and enterprise 5G services such as augmented reality and content distribution at low cost, low latency, and high accuracy.

Fredrik Jejdling, executive vice-president and head of business area networks, Ericsson, says: “We continue to focus our efforts on helping our customers succeed with 5G.

“These new solutions will allow them to follow the 5G evolution path that fits their ambitions in the simplest and most efficient way.”

Ericsson says the new standalone 5G NR software can be installed on its existing Radio System hardware.

Coupled with Ericsson’s 5G dual-mode Cloud Core solutions, the new products are aimed at opening new business opportunities for service providers – especially having established an architecture that facilitates agility, provides advanced support for network slicing and enables the speedy creation of new services.

Ericsson says most operators will start with NSA and once the 5G coverage has been established, also deploy standalone.

“Low bands will play a key role in cost-efficiently extending the coverage provided by 5G deployments to date.

“Ericsson has also launched Inter-band NR Carrier Aggregation – a new software feature that extends the coverage and capacity of NR on mid- and high bands when combined with NR on low bands.

“This will improve speeds indoors and in areas with poor coverage.

“Two new Massive MIMO radios have also been added to the Ericsson Radio System mid-band portfolio, allowing service providers to build 5G with precision.

“5G enables augmented reality, content distribution and gaming, and other applications that require low latency and high bandwidth to perform with accuracy.

“To help service providers meet these requirements and offer new consumer and enterprise services, Ericsson is evolving its cloud solution with the launch of Ericsson Edge NFVI (Network Functions Virtualisation Infrastructure), optimised for the network edge.

“A compact and highly efficient solution, Ericsson Edge NFVI is part of the end-to-end managed and orchestrated distributed cloud architecture, which makes it possible to distribute workloads, optimise the network and enable new services in the cloud,” Ericsson said.

Ericsson also announced it would be launching its VNF Certification Service, a partner certification program for virtual network functions.

The company said the service is open to all VNF vendors and grants a certification on the Ericsson NFVI platform using Ericsson Labs, which will create an ecosystem with a shorter time-to-market for working with partners and applications.

Industry Analyst Hugh Ujhazy, vice-president, IOT & Telecommunications at International Data Corporation, Asia Pacific, says: “Ericsson’s latest 5G offerings equip service providers with an even broader 5G portfolio by adding the Standalone NR option.

“The series of solutions being added to the Ericsson 5G platform will allow service providers to deploy 5G sensibly and address new business opportunities with full flexibility.

“What you get is faster, cheaper, makes better use of existing assets and with fewer truck rolls. That’s pretty cool.”

Peter Dinham

ANDROID MALWARE BYPASSES GOOGLE PERMISSIONS RESTRICTIONS

Android malware has been discovered that sidesteps measures introduced by Google in March, to restrict the use of SMS and Call Log permissions preventing apps from abusing these permissions and bypassing SMS-based two-factor authentication.

In **a blog post**, a researcher from Slovakian security firm ESET, Lukas Stefanko, said the new malicious apps were able to access one-time passwords in SMS two-factor messages without using any SMS permissions.

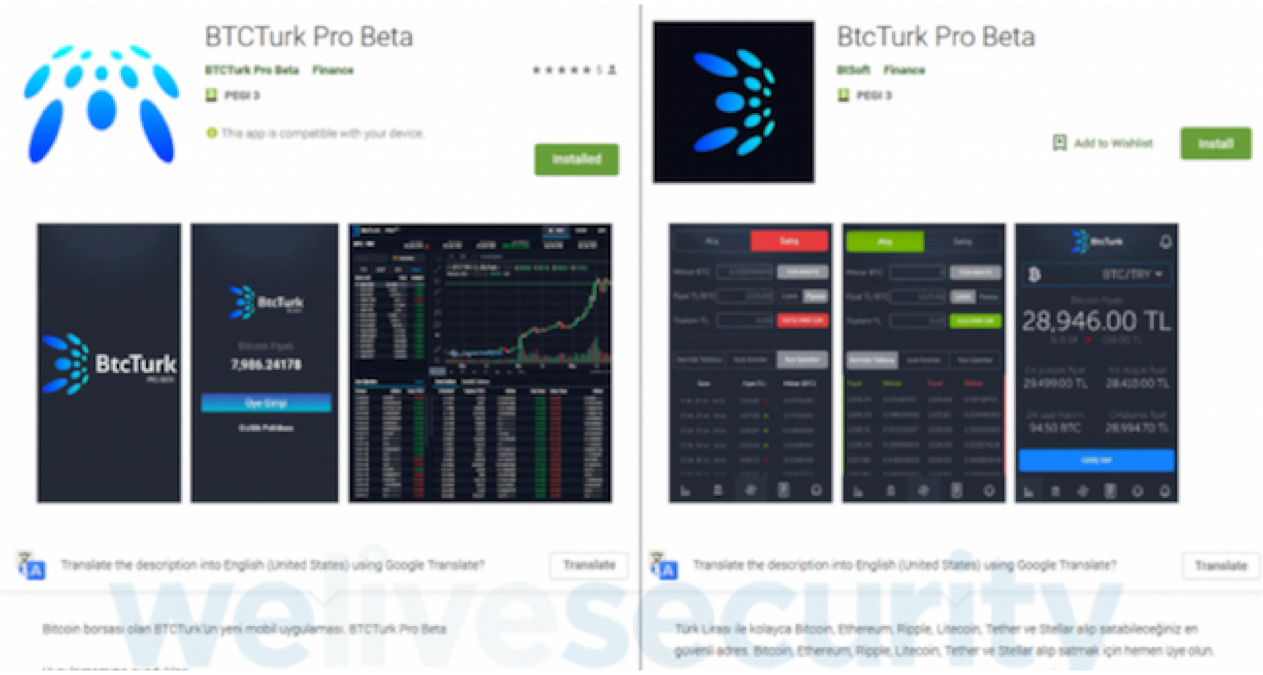
"As a bonus, this technique also works to obtain OTPs from some email-based 2FA systems," he said.

The apps were built to pass as the Turkish cryptocurrency exchange BtcTurk and used phishing to obtain login credentials to the exchange.

Rather than intercept an SMS to bypass 2FA protection, the apps took the OTP from notifications that appeared on the display of a compromised display.

"The first of the malicious apps we analysed was uploaded to Google Play on 7 June as 'BTCTurk Pro Beta' under the developer name 'BTCTurk Pro Beta'," Stefanko said.

"It was installed by more than 50 users before being reported by ESET to Google's security teams."



Translate the description into English (United States) using Google Translate?

Bitcoin borsası olan BTCTurk'ün yeni mobil uygulaması. BTCTurk Pro Beta

Translate the description into English (United States) using Google Translate?

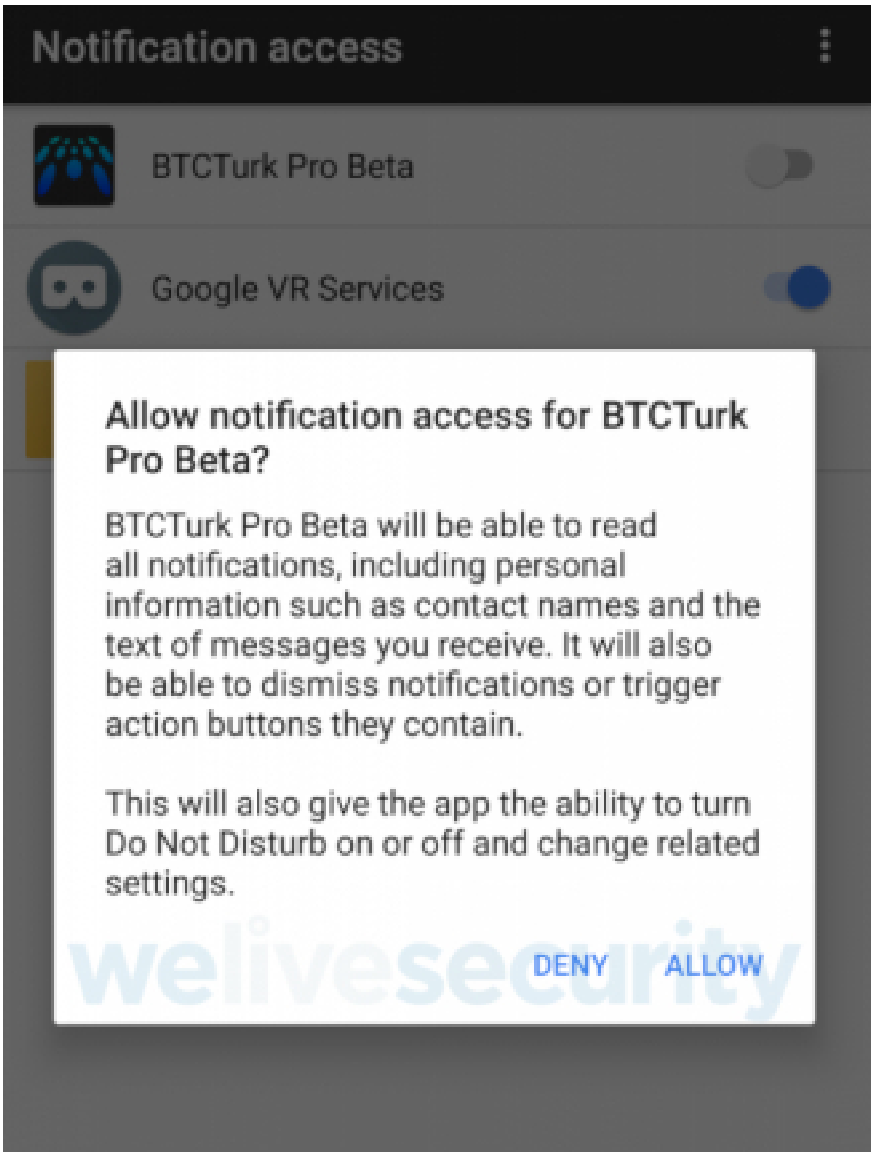
Türk Lirası ile kolayca Bitcoin, Ethereum, Ripple, Litecoin, Tether ve Stellar alıp satabileceğiniz en güvenli adres. Bitcoin, Ethereum, Ripple, Litecoin, Tether ve Stellar alıp satmak için hemen üye olun.

The two apps seen in the Play Store.

A second app was uploaded four days later, with a subtle difference; the name was BtcTurk Pro Beta and the developer's name was given as BtSoft.

This app was reported to Google on 12 June before even 50 users could install it.

Stefanko said once either app was launched, it asked for a permission named Notification access (below).



Allow notification access for BTCTurk Pro Beta?

BTCTurk Pro Beta will be able to read all notifications, including personal information such as contact names and the text of messages you receive. It will also be able to dismiss notifications or trigger action buttons they contain.

This will also give the app the ability to turn Do Not Disturb on or off and change related settings.

"This permission allows the app to read the notifications displayed by other apps installed on the device, dismiss those notifications, or click buttons they contain," he added.

Once this was granted, the app showed a fake login asking for credentials to log in to BtcTurk. Once these were entered, they were sent to attacker's server, and a fake error message in Turkish displayed on the device.

Stefanko said users could avoid getting caught by apps of this kind by trusting cryptocurrency-related and other finance apps only if they were linked from the official website. Another tip he offered was to only allow Notification access to those apps that had a legitimate reason for requesting it.

Sam Varghese

ISRAELI FIRM CELLEBRITE SAYS IT CAN HACK IOS 12.3 DEVICES

Israeli firm Cellebrite, widely believed to be the company that helped the FBI bypass Apple and gain access to the iPhone of a terrorist in 2016, has advertised its latest wares as being able to break into systems running iOS 12.3 and also recent Android phones.

Cellebrite **said** it was able to bypass or determine the locks and also perform a full file extraction on any iOS device.

The company also said it was able to perform a physical extraction or full-file system extraction on many high-end Android devices.

"Gain access to 3rd party app data, chat conversations, downloaded emails and email attachments, deleted content and more, increase your chances of finding the incriminating evidence and bringing your case to a resolution," it said in a marketing plug.

In April 2016, it was **reported** that Cellebrite was paid more than US$15,000 for breaking into the iPhone of Syed Rizwan Farook, one of two terrorists involved in an attack in San Bernardino, California, in December 2015.

But in May 2017, Democrat senator Dianne Feinstein **revealed** that the FBI paid a private company US$900,000 to break the encryption on the iPhone 5C.

Later that same year, it was reported that the Australian Taxation Office had **paid** Cellebrite $42,747 for training its employees in using software for breaking into mobile devices.

And in June 2017, another **report** said many government agencies, including ASIC, the AFP, and the Department of Defence, were using Cellebrite's services.

On its website, Cellebrite said it offered support for Apple devices running iOS 7 to iOS 12.3. It also offered support for Android models, including the Galaxy S6, S7, S8 and S9 models.

Apart from this, the company also said its software would work with popular models from Motorola, Huawei, LG and Xiaomi.

Sam Varghese