When Chinese Networks Spy On
Users

May 07, 2019

By Jeff Ferry, CPA Chief Economist

On April 30th, global wireless telecom company Vodafone went public with a statement to Bloc
London-based wireless provider found “hidden backdoors,” i.e. multiple security flaws in the w
Chinese network provider Huawei.

The problem first surfaced in 2011 when Vodafone engineers found “backdoors” in Huawei brc
equipment in their Italian network. Backdoors are software access points which allow the netw
case), or third parties like hackers or spies, to get into the network and potentially see the priva
users.

According to Bloomberg and a more in-depth report in British technology publication The Regi in 2011 found that Huawei routers had a "hidden" backdoor that could be used by a malicious that router but of the entire network. Huawei told Vodafone it would remove the backdoor. Ho Vodafone later that year found it was still there. When Vodafone protested, Huawei then chang backdoor needed to remain for network management purposes.

Vodafone Chief Information Security Officer Bryan Littlefair wrote up the situation this way in a concern here is that actions of Huawei in agreeing to remove the code, then trying to hide it, ar they need it to remain for `quality' purposes."

African Union

The story of spying at the African Union (AU) headquarters offers an equally worrying tale. A de provider built a network in the new headquarters of the African Union in Addis Ababa, Ethiopia for the 55 nations of Africa to work together. The new 19-story glass tower headquarters (abov Construction Engineering Corporation. The name of the network provider has not been reveale companies capable of providing a full-service wireline and wireless network are Huawei and ZT provided voice, video, and data services within the headquarters and high-speed connections t

According to a shocking article in French newspaper Le Monde published on January 26, 2018, managers discovered in 2017 that the network was a giant listening device. Wrote Le Monde: "a sources, each night the secrets of this institution were copied and stored more than 8,000 kilo mysterious servers hosted somewhere in Shanghai."

The espionage began in 2012 and continued nightly until 2017, when Union technology manag According to Le Monde and the London Financial Times (FT), which independently confirmed th avoid embarrassment by replacing the Chinese technology while publicly denying the espionag tech team added encryption to all their communications and stopped using Ethio Telecom, whi electronic surveillance. According to Le Monde, when the Chinese engineers offered to configu managers thanked them politely—but did it themselves instead.

One angry senior African Union official told Le Monde: "We let them bug us and we did nothing hours out of 24. They planted lots of microphones and cyber-spying tools when they built the b

The FT pointed out that China has built much of the modern infrastructure across Africa, relyin investment budget President Xi pledged for Africa three years ago. That infrastructure includes telecom networks. Quoting a McKinsey report, the FT said there are 10,000 Chinese companies

Writing for the Council of Foreign Relations, Africa analyst Mailyn Fidler commented last year th to address China's behavior demonstrates just how dramatically China's influence has narrowe

this continues, African autonomy will take a real hit."

In another media investigation, British technology publication The Register revealed that Huaw vulnerability in the software code in its broadband gateways (home routers) back in 2013, but t correct the problem. Huawei created a software patch to fix the problem on that specific mod software on all its broadband gateways. The result was that four years later, in 2017, Israeli Int Point Research found that the vulnerability was being exploited by a hacker known as Nexus Z plant the Mirai virus on Huawei home routers in the US, Italy, Egypt, and elsewhere. That virus actors to take out large sections of the Internet—although in this case no major outages were r

It's not clear whether Huawei dragged its feet on upgrading its broadband gateway software ou it had a hidden agenda for using that vulnerability. The Register sees it as "bungling" by the Chi recent summary of the affair, The Register made clear its doubts about Huawei's reliability: "Bri while Huawei network equipment is not secure enough for government networks, officials say general public to the potential risks present in Huawei gear."

The problem for the UK, US, and other non-Chinese governments is that there is a very limited providers. A telecom company's relationship with its network provider is akin to a marriage. Th demanding before it selects its network provider, but once it has agreed to work with a networ stuck with each other for years. A nationwide telecom network can easily cost over $100 millio install.

Even though the telecom company is the customer and writing the checks, once the network is telecom company can find it hard to get the network provider to do what it wants, as quickly as changes or upgrades becomes a major engineering project. (Here's another reportfrom Britain Huawei.) For this reason, telecom companies always want to have two providers in their netwo alternative in case the situation gets bad enough that the telecom company wants either to thr "rip and replace" to throw out one network provider.

Aside from Huawei, there are only two truly full-service wireline and wireless network provider of Sweden. US allies like Britain and Germany have refused to go along with the US request to major networks partly because a third provider is a very useful weapon to keep the other two p are always a subject of negotiation, timing issues are often more contentious. The telecom cus be they installations, upgrades, or fixes, to be completed quickly; the network provider often se than the customer would like and then falls behind its own schedule.

The British government's decision to allow its large carriers to use Huawei in non-core parts of to offer a sop to Washington while at the same time allowing British telecom companies to kee as a bargaining tool.

As the above events show, this sort of compromise solution is likely to please neither the US go telecom companies. It's also unlikely to deliver a truly secure service to local network users. Th alternative provider, preferably one based in the US. A $50 billion-plus a year market can supp

See also this [2018 article on Chinese IP theft]

Be The First To Comment

Sign in with

Facebook

Twitter

Or sign in with email

Email Address

Password

Remember me

POST YOUR COMMENT

or Create an account

Custom Search

NAVIGATE

Who We Are
Act
Press
Attend
Member Login

SOCIAL MEDIA

CONTACT US

PHONE: **202.688.5145**
EMAIL:
info@prosperousamerica.o

Website by VOXARA