EXCLUSIVE: US hacked Pacnet, Asia Pacific fibre-optic network operator, in 2009

According to information provided by Edward Snowden to the Post, computers owned by Pacnet in Hong Kong were attacked by the US National Security Agency in 2009, but the operation has since been shut down

Computers at the Hong Kong headquarters of Pacnet – owner of one of the biggest fibre-optic networks in the region – were hacked by US spies in 2009, adding fuel to the diplomatic fire that has engulfed the Obama administration this month over its cyber-snooping activities worldwide.

According to information provided by Edward Snowden to the *Post*, computers owned by Pacnet in Hong Kong were attacked by the US National Security Agency but the operation has since been shut down.

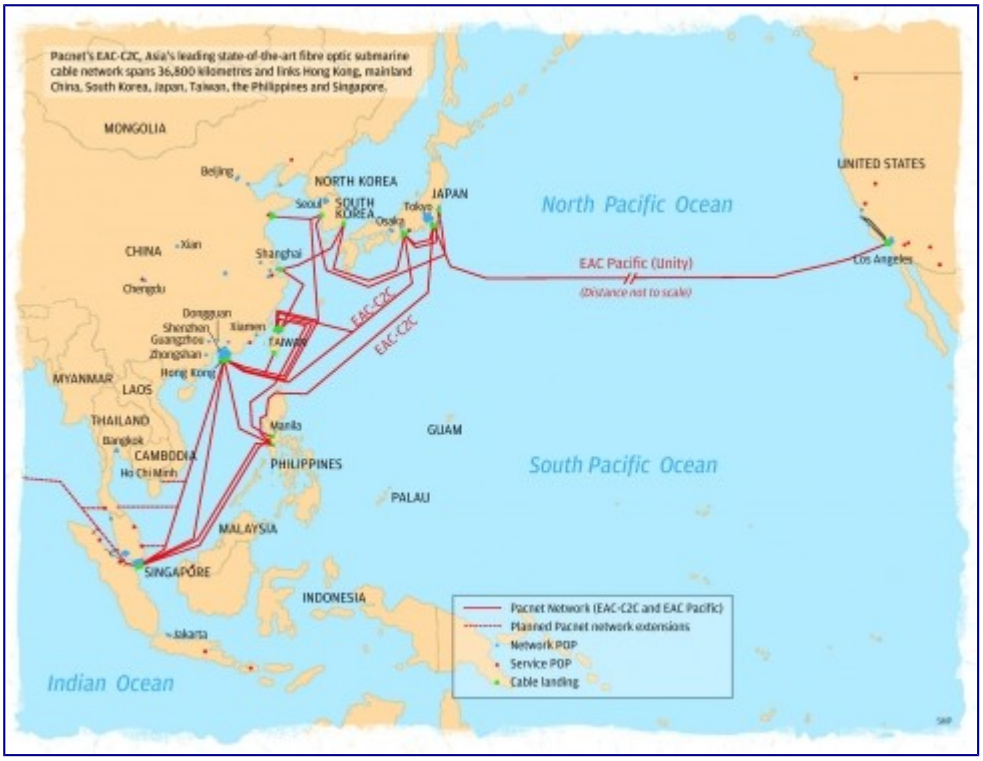
The latest revelations come as the scope of cyber-spying by US and UK secret agents widened with new reports by *The Guardian* newspaper claiming the UK spy agency, GCHQ has the means to tap into a wealth of data held in fibre-optic cables.

Last week, Snowden made the explosive claim that hundreds of computers in Hong Kong and mainland China had been targeted by the NSA over a four-year period.
The information on the attacks on Pacnet are based on a range of details including dates, domain names, internet protocol numbers and other operational details provided by Snowden.

If the legal system in a country allows for tapping into fibre-optic connections, there is little control over it at the other end.
Prof. Chow Kam-pui, HKU

Pacnet, which has global headquarters in Hong Kong and Singapore, owns more than 46,000 kilometres of fibre-optic submarine cables and provides connections to 16 data centres for telecom companies, multinationals and governments across Asia Pacific.

Its regional network spans Hong Kong, the mainland, Korea, Japan, Taiwan, the Philippines and Singapore.



Pacnet has five data centres on the mainland with the most recent opening last December in Tianjin.

It also has offices in the Netherlands and the US.

Last Thursday, Pacnet announced that its joint venture in China, Pacnet Business Solutions, had signed new deals with the three major mainland telecom providers: China Telecom, China Unicom and China Mobile.

Pacnet said its service agreements with the three companies would see it provide "border gateway protocol" services to the firms. Broadly speaking , the "border gateway protocol" is the protocol which ties the internet together.

The move allows the company to service global cloud computing providers who want to set up on the mainland.

The claims about the NSA hacking into computers such as Pacnet's follows on from last week's revelation that the Chinese University of Hong Kong had been targeted by the spy agency. Snowden says that the US is targeting "network backbones" through which large quantities of data pass.

The university is home to the Hong Kong Internet Exchange, a comprehensive infrastructure hub through which all the city's internet traffic passes.

After Snowden's claims were made public by the *Post*, Hong Kong Secretary for Security Lai Tung-kwok announced that police had checked the hub and that the government had set up round-the-clock monitoring of the exchange.

Chinese University says it checked its servers and had not detected any attacks, but it did not specify between what period it had investigated.

According to its official website, Pacnet owns and operates the leading pan-Asian submarine cable network and has a presence at 19 cable landing stations, extending from India to the US.

In January 2008, the company was rebranded Pacnet after a merger between Asia Netcom and Pacific Internet, which the company claimed made it the communications firm with the largest regional footprint and the most extensive submarine cable infrastructure. Pacnet is privately owned. According to its website its ownership includes London-based Ashmore Investment Management and Clearwater Capital Partners of New York. Reuters reported in January last year that the owners' plans to sell the company had stalled due to lower than expected bids.The majority of fibre-optic connections in Hong Kong lead to the United States because some of the most important internet services – such as the domain name service, some popular cloud computing services and search engines like Google and Yahoo – have their roots in the US, said professor Chow Kam-pui, associate director of the Computer Forensics Research Group at the University of Hong Kong. "If you're on the internet, you would be using fibre-optic connections to the US most of the time," he said.

He said if the NSA tapped into fibre-optic connections it would probably do so at the American end, he said. Tapping into the connections at the Hong Kong end would need physical access to the system, he added.

"If the legal system in a country allows for tapping into fibre-optic connections, there is little control over it at the other end," he said.
The claims that the NSA has been hacking into computers with links to fibre-optic networks comes as new Guardian reports reveal that Britain's Government Communications Headquarters had secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American counterpart. The documents show that one key innovation was that the data could be drawn from cables for up to 30 days so it could be sifted and analysed.

That operation, codenamed Tempora, has been running for some 18 months, *The Guardian* reported.

The types of data collected ranged from recordings of phone calls, email messages, Facebook entries and the history of any internet user's access to websites.

“It’s not just a US problem. The UK has a huge dog in this fight,” Snowden told the *Guardian*. “They [GCHQ] are worse than the US.”

The Guardian’s report said a source with knowledge of intelligence argued that the data was collected legally under a system of safeguards, and had provided material that had led to significant breakthroughs in detecting and preventing serious crime.

UK officials could also claim GCHQ “produces larger amounts of metadata than NSA”. (Metadata describes basic information on who has been contacting whom, without detailing the content.) The documents reveal that by last year GCHQ was handling 600m “telephone events” each day, had tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time.

Additional reporting by Jennifer Ngo and the Guardian

This article appeared in the South China Morning Post print edition as Cyberspies tapping global data cable operators

Original:
http://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator

22 June 2013 – South China Morning Post