GlobalResearch
Center for Research on Globalization

# Snake-Oil Alert – Encryption Does Not Prevent Mass-Snooping

By Moon of Alabama
Global Research, March 11, 2017
Moon of Alabama 9 March 2017

Region: USA
Theme: Intelligence, Police State & Civil Rights

*The WikiLeaks stash of CIA hacking documents shows tools used by the CIA to hack individual cell-phones and devices. There are no documents yet that suggest mass snooping efforts on a very large scale. Unlike the NSA which has a "collect it all" attitude towards internet traffic and content the CIA seems to be more interested in individual hacking.*

This suggests that the CIA can not decipher the modern encrypted communication it adversaries use. It therefore has to attack their individual devices.

But it does not mean that the CIA can not engage in mass snooping.

The New York Times description is wrong:

> Some technical experts pointed out that while the documents suggest that the C.I.A. might be able to compromise individual smartphones, there was no evidence that the agency could break the encryption that many phone and messaging apps use.If the C.I.A. or the National Security Agency could routinely break the encryption used on such apps as Signal, Confide, Telegram and WhatsApp, then the government might be able to intercept such communications on a large scale and search for names or keywords of interest. But nothing in the leaked C.I.A. documents suggests that is possible.
>
> Instead, the documents indicate that because of encryption, the agency must target an individual phone and then can intercept only the calls and messages that pass through that phone. Instead of casting a net for a big catch, in other words, C.I.A. spies essentially cast a single fishing line at a specific target, and do not try to troll an entire population.
>
> "The difference between wholesale surveillance and targeted surveillance is huge," said Dan Guido, a director at Hack/Secure, a cybersecurity investment firm. "Instead of sifting through a sea of information, they're forced to look at devices one at a time."

Snake-oil alert: Right diagnosis, wrong conclusion and therapy.


If the CIA breaks into an individual Samsung Galaxy 7 it can record what is typed on the screen, and whatever gets transferred via the microphone, camera and loudspeaker. No encryption can protect against that. But why should the CIA break into only one Galaxy 7?

It is wrong to conclude that the CIA can therefore not “intercept such communications on a large scale”. It can. Easily.

If you can break into one individual Samsung Galaxy 7 you can break into all of them. This can be automated.

The CIA also breaks into internet routers and network infrastructure systems. By watching the network traffic flowing by the CIA (and NSA) systems can “see” who uses encrypted communication. They can then launch programs to silently take over the communicating devices. Then the communication can be recorded from the devices and read in the clear. There is nothing at all that prohibits this to take place on a massive scale.

The reaction to the Snowden leaks about gigantic NSA snooping on internet lines led to an increased use of encryption. Suddenly everyone used HTTPS for web traffic and the user numbers of Signal, Telegram, WhatsApp and other encrypting communication applications exploded.

But encrypted traffic still sticks out. One can detect an encrypted skype call by watching the network traffic on this or that telecom network. One can detect what kind of end-devices are taking part in a specific call. With a library of attack tools for each of the usual end-devices (Iphone, Android, Windows, Mac) the involved end-devices can be silently captured and the call can be recorded without encryption.

The Times writes: “Instead of casting a net for a big catch, in other words, C.I.A. spies essentially cast a single fishing line at a specific target, and do not try to troll an entire population.”

It is right in one sense. There is not one central point in the river of traffic where one casts the net. But it is wrong in to conclude that the CIA or other services would then use “a single fishing line”. What hinders them from using hundreds of fishing lines? Thousands? Hundred-thousands?

Wide use on encryption simply moves the snooping efforts from the networks towards the end-devices. It might be a little more expensive to snoop on hundred-thousands of end-

devices than on a few network backbones but budget or manpower restriction are not a problem the NSA and CIA have had in recent decades.

To tell users that it encryption really restricts the CIA and NSA is nonsense. Indeed it is irresponsible.

The sellers of encryption are peddling snake-oil. The dude from “a cybersecurity investment firm” the Times quotes is just selling his rancid wares.

Your neighbor snoops on your open WLAN traffic? Yes, chat encryption might prevent him from copying your session with that hot Brazilian boy or girl. But it does not prevent professionals from reading it. For that you would need secure devices on both ends of the communication. Good luck finding such.



---