

Encrypted Blackphone goes to war with snoopers

January 19 2014, by Rob Lever



Mike Janke, CEO & Co-Founder of Silent Circle, makers of encrypted technology for mobile and desktop devices and email, stands January 16, 2014, at his National Harbor, Maryland office

It's a fully encrypted smartphone that aims to foil snooping governments, industry rivals and hackers.

It's also a sleek, attractive device that fits in your pocket and can impress friends and colleagues, according to its makers.

The Blackphone is set to be released next month by the secure communications firm Silent Circle and the small Spanish-based manufacturer Geeksphone, amid a fever pitch of concern over revelations about vast US surveillance of data and telephony.

But Silent Circle chief executive Mike Janke said his company was working on the handset even before last year's revelations about the wide-ranging US National Security Agency programs, leaked by former contractor Edward Snowden.

"We did this because there was a problem that was not being solved: [secure communications](#)," Janke told AFP in an interview in the Silent Circle offices overlooking the Potomac River just outside Washington.

Silent Circle was formed in 2011 and in 2013 launched apps and other services which allow smartphone and PC users to send encrypted messages and videos.

The Blackphone is an extension of that effort, says Janke, a former Navy SEAL who co-founded the firm with other ex-SEALs and Silicon Valley cryptographic experts.

"We offer completely encrypted, peer-to-peer communications. We have encrypted video, encrypted text and secure VoIP (Voice-over-Internet-Protocol) calls," Janke said.

The founders include Phil Zimmermann, who created the widely used PGP (Pretty Good Privacy) standard, and former Apple cryptographic expert Jon Callas.

Last year, Silent Circle halted its encrypted email service to avoid becoming a target after the US government subpoenaed the records of a similar service called Lavabit.

"We destroyed all that data," said Janke, while adding that the company never faced a subpoena.

Silent Circle customers include major global corporations, human rights activists and even the Tibetan government in exile.

Because of its work, he said, "almost all of the major smartphone manufacturers came to us" to collaborate on a more secure smartphone.

Janke said Silent Circle chose to form a joint venture for Blackphone with the small Spanish company which recently began making smartphones using the Firefox operating system.

The larger firms, said Janke, "want to own your soul. These companies are in the business of monetizing data."

Silent Circle developed a modified or "forked" version of Android called PrivatOS for the phone, which is set to be unveiled at Mobile World Congress in Barcelona on February 24.

'It's sexy, it's thin'

The company declined to release detailed specifications or pricing ahead of the unveiling, but Janke said it will be sold around the world at prices lower than the iPhone 5S or Samsung Galaxy S4.

But he maintained it would be comparable in terms of performance to those flagship devices. It is designed as a user-friendly phone that could be carried by executives, government officials, activists or ordinary

people.

"It's sexy, it's thin, it's sleek, but it also solves a problem," Janke said.

"You can still go to Google and browse the web, but Google doesn't know who you are. It's a high-end smartphone. The user doesn't have to know how to use or how to spell encryption."

As an added assurance to customers, the Blackphone venture is incorporated in Switzerland with a Swiss data center and has "minimal data retention."

"All we have is the user name you give us and a 10-digit phone number," he said.

Even if the company faced a court order in Switzerland, it could only hand over the user name. Authorities seeking more information would need to subpoena a separate payment processing firm "and try to match that to our users," Janke said.

Janke said there is interest in the device worldwide, and that Blackphone has "verbal pre-orders" from four international telecom carriers and 30 enterprise customers.

Interest in Blackphone, Janke said, suggests "several million" will be sold within 12 months, and some 10 million total over the coming four years.

He did not disclose where the Blackphone would be made, but said there would be "neutral" partners making components and a tightly controlled assembly process to ensure no backdoors are inserted.

Janke said the US State Department wanted to buy some of the phones and distribute them to human rights groups but that the company

refused, out of concern that the Blackphone would be associated with the US government.

"We decided to distribute this ourselves," he said.

Customers worldwide are interested "because it's not just the NSA—there are 72 countries that have some NSA-like capabilities and they're all spying on us and on each other. If you're living in Kenya or Germany or Argentina, you have the same threats."

Even though some reports suggest the NSA has found ways to intercept encrypted communications, Janke said his systems will be effective.

"We know that encryption works," he said, adding that "brute force" attacks to break encryption are rare because they are time-consuming, and that spy agencies generally use other means like inserting viruses in emails or hardware that can intercept messages.

Because of this, Janke is careful not to promise too much. He said Blackphone is not a "hardened" device like some designed for military use.

"There is no such thing as a completely secure phone," he said. "Nothing is going to protect you from your own behavior. But out of the box, this phone does a lot of things to protect your privacy."

© 2014 AFP

Citation: Encrypted Blackphone goes to war with snoopers (2014, January 19) retrieved 10 April 2024 from <https://phys.org/news/2014-01-encrypted-blackphone-war-snoopers.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.