The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Defense Contractor Developing Smartphone Spyware, U.S. Firm Says

By Reuters

July 24, 2019

Mikhail Metsel / TASS

A Russian defense contractor accused by the United States of supporting cyberattacks has developed sophisticated software used to spy on smartphones, an American security company said on Wednesday.

St. Petersburg-based Special Technology Center (STC) developed code that has been aimed at a small number of targets, including those interested in a rebel militia in Russian-allied Syria, security firm Lookout said in a report.

Lookout, which specializes in securing mobile devices against cyberattacks, said it detected samples of the malware aimed at phones running Google's Android almost a year ago.

It declined to say whether the samples were found on its users' phones or in what country the attacks had been detected.

Related article: Western Intelligence Hacked 'Russia's Google' Yandex to Spy on Accounts

The United States and other Western countries have accused the Russian government and companies working on its behalf of conducting cyberattacks against organizations around the world.

The Kremlin has repeatedly denied the allegations, which it says are not supported by real evidence and did not immediately respond to a request for comment on Lookout's findings.

STC did not immediately respond to a request for comment either.

Investigators at Lookout, which is headquartered in San Francisco and produces mobile security software for U.S. government agencies as well as consumers, said they had named the spyware Monokle after a term found in the code.

'Malicious activities'

Monokle can be remotely operated, they said, and communicated with an Internet Protocol address that was also used to send commands to defensive software made by STC.

"Monokle is an advanced and full-featured piece of surveillanceware which has implemented several features we haven't seen before to capture data," Lookout said.

The program can be installed on victims' devices in multiple ways, including through corrupted versions of popular apps. In some cases, it installed certificates that allowed it to intercept encrypted internet traffic.

It also tried to capture user codes for unlocking the devices.

The United States sanctioned STC and two other companies in 2016 for engaging in "malicious cyber-enabled activities," including providing support to the Russian military intelligence agency. STC is better known for manufacturing drones and other equipment for the Russian military.

Spyware aimed at phones is a varied and competitive field, with sophisticated versions like Monokle sold to national governments, turnkey hacking services sold to police and cheap "spouseware" sold to individuals tracking their romantic partners or family members, often illegally.

Vendors at all levels have suffered hacks in recent years, including some who sold high-end tools to the West, by anonymous people claiming to act for moral reasons. Meanwhile, Russia has been accused by U.S. authorities of stealing hacking tools directly from American agencies.

Original url:
https://www.themoscowtimes.com/2019/07/24/russian-defense-contractor-developing-smartphone-spyware-us-firm-says-a66556