The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

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

By Reuters

June 27, 2019

Hackers working for Western intelligence agencies broke into Russian internet search company Yandex in late 2018 deploying a rare type of malware in an attempt to spy on user accounts, four people with knowledge of the matter told Reuters.

The malware, called Regin, is known to be used by the "Five Eyes" intelligence-sharing alliance of the United States, Britain, Australia, New Zealand and Canada, the sources said. Intelligence agencies in those countries declined to comment.

Western cyberattacks against Russia are seldom acknowledged or spoken about in public. It could not be determined which of the five countries was behind the attack on Yandex, said sources in Russia and elsewhere, three of whom had direct knowledge of the hack. The breach took place between October and November 2018.

Yandex spokesman Ilya Grabovsky acknowledged the incident in a statement to Reuters, but declined to provide further details. "This particular attack was detected at a very early stage

by the Yandex security team. It was fully neutralized before any damage was done," he said.

The company, widely known as "Russia's Google" for its array of online services from internet search to email and taxi reservations, says it has more than 108 million monthly users in Russia. It also operates in Belarus, Kazakhstan and Turkey.

The sources who described the attack to Reuters said the hackers appeared to be searching for technical information that could explain how Yandex authenticates user accounts. Such information could help a spy agency impersonate a Yandex user and access their private messages.

The hack of Yandex's research and development unit was intended for espionage purposes rather than to disrupt or steal intellectual property, the sources said. The hackers covertly maintained access to Yandex for at least several weeks without being detected, they said.

The Regin malware was identified as a Five Eyes tool in 2014 following revelations by former U.S. National Security Agency (NSA) contractor Edward Snowden.

Reports by The Intercept, in partnership with a Dutch and Belgian newspaper, tied an earlier version of Regin to a hack at Belgian telecom firm Belgacom in 2013 and said British spy agency Government Communications Headquarters (GCHQ) and the NSA were responsible. At the time GCHQ declined to comment and the NSA denied involvement.

'Crown Jewel'

Security experts say attributing cyber attacks can be difficult because of obfuscation methods used by hackers.

But some of the Regin code found on Yandex's systems had not been deployed in any known previous cyber attacks, the sources said, reducing the risk that attackers were deliberately using known Western hacking tools to cover their tracks.

Yandex called in Russian cybersecurity company Kaspersky, which established the attackers were targeting a group of developers inside Yandex, three sources said. A private assessment by Kaspersky, described to Reuters, concluded hackers likely tied to Western intelligence breached Yandex using Regin.

Related article: Russia's Yandex Pushes Back Against Pressure to Share Encryption Keys

Yandex called in Russian cybersecurity company Kaspersky, which established the attackers were targeting a group of developers inside Yandex, three sources said. A private assessment by Kaspersky, described to Reuters, concluded hackers likely tied to Western intelligence breached Yandex using Regin.

A Kaspersky spokeswoman declined to comment.

The U.S. Office of the Director of National Intelligence declined to comment. The White House National Security Council did not respond to a request for comment.

Kremlin spokesman Dmitry Peskov said the Russian government was not aware of this particular attack on Yandex. "Yandex and other Russian companies are attacked every day. Many attacks come from Western countries," he said.

Moscow-based Yandex, a privately held company listed on the NASDAQ in the United States and the Moscow Exchange, has come under tighter regulatory control by the Russian government after the passage of new internet laws. Former Russian economics and trade minister Herman Gref became a Yandex board member in 2014.

U.S. cybersecurity firm Symantec said it had also recently discovered a new version of Regin. Symantec declined to discuss where this sample was discovered, citing client confidentiality.

"Regin is the crown jewel of attack frameworks used for espionage. Its architecture, complexity and capability sits in a ballpark of its own," Vikram Thakur, technical director at Symantec Security Response, told Reuters. "We have seen different components of Regin in the past few months."

"Based on the victimology coupled with the investment required to create, maintain, and operate Regin, we believe there are at best a handful of countries that could be behind its existence," said Thakur. "Regin came back on the radar in 2019."

Original url:
https://www.themoscowtimes.com/2019/06/27/western-intelligence-hacked-russias-google-yandex-to-spy-on-accounts-a66194