Russian digital services provider targeted by Western intelligence agencies

Reference: Memo [190701-1] Date: 01/07/2019 - Version: 1.1
Keywords: telecoms, espionage, Russia, United States, United Kingdom
Sources: publicly available information

Key Points

- According to open sources, hackers breached the systems of Russian digital service provider Yandex.
- The breach occurred between October and November 2018.
- According to Reuters, the cyber intruders used the Regin espionage malware.
- Previous Regin attacks (Belgacom case publicly uncovered in 2014) have been attributed to US and British intelligence agencies by open sources.

Summary

On June 27, Reuters reported that hackers likely to be working for Western intelligence agencies breached the systems of the Russian digital services giant Yandex. The breach occurred between October and November 2018 and involved a new variant of the sophisticated Regin malware. The attack was reported to Reuters by four undisclosed sources. It specifically targeted Yandex's research and development unit. Its goal was likely to steal technical information on the company's user authentication system. This information may have allowed the attackers to impersonate Yandex users and obtain their private messages.

Yandex spokesman Ilya Grabovsky acknowledged the incident and said: "This particular attack was detected at a very early stage by the Yandex security team. It was fully neutralized before any damage was done. The Yandex security team's response ensured that no user data was compromised by the attack."

According to Reuters, Yandex hired the Russian cybersecurity company Kaspersky to analyse the incident. An assessment by Kaspersky reportedly concluded that hackers likely tied to Western intelligence breached Yandex using a Regin variant.

Comments

Regin is a sophisticated cyber-espionage framework that was used in the attack against Belgacom which was publicly revealed in 2014. Several sources have attributed this attack to US and British (GCHQ) intelligence agencies. In an analysis released in 2014, Symantec stated that "Regin infections [had been] observed in a variety of organisations between 2008 and 2011, after which it was abruptly withdrawn. A new version of the malware resurfaced from 2013 onwards. Targets include private companies, government entities and research institutes. Almost half of all infections targeted private individuals and small businesses. Attacks on telecoms companies appear to be designed to gain access to calls being routed through their infrastructure." In August 2015, Symantec revealed the existence of 49 new modules of the Regin espionage platform. Open source reporting states that Regin has been mostly used against Russian and Saudi Arabian targets with four EU countries being among the most common targets.

Yandex N.V. is a Russian multinational business providing Internet-related products and services, including search and information services, eCommerce, transportation, navigation, mobile applications, and online advertising. It is the largest technology company in Russia and the largest search engine on the internet in Russian.

Recently, Russia has introduced new legislation related to its digital infrastructure and services. The aim is to reinforce its strategic autonomy and to improve the independence and the resilience of the Russian segment of the internet dubbed RUNET (see CERT-EU Threat Landscape Reports 2019Q1 and Q2). According to the legislation, RUNET should continue functioning even if it was disconnected from the global internet structure. Russian telecom providers should minimise the flow of internet traffic to servers outside of Russia's borders when it contains communications between Russian citizens. The discussions around new legislation also propose a new Russian national domain name system. The Ministry of Communications and Mass Media (Minkomsvyaz) has named three threats to communication networks that would act as catalysts to isolate the Russian segment of the internet (RUNET) and allow the domestic internet watchdog Roskomnadzor to assume control of RUNET: (1) integrity threats (impossibility to connect users), (2) stability threats (equipment failure, natural or man-made disaster), (3) security threats (when a provider cannot counter attempts to hack equipment or disrupt networks). Authors of the new legislation say Russia must ensure the security of its networks after the US president, Donald Trump, unveiled a new US cybersecurity strategy last year that said Russia had carried out cyber-attacks with impunity.