Russian FSB's projects leaks by hacktivists

Reference: Memo [190730-1] – Version: 1.0
Keywords: FSB, SyTech, ov1ru$, DigitalRevolution
Sources: Publicly available information

Key Points

- Russian FSB's contractor SyTech was reportedly hacked and 7.5TB of data were leaked.
- This leak contains information about at least 20 FSB's digital monitoring projects.
- A Russian-speaking hacktivist group dubbed the DigitalRevolution group is involved in the leak.

Summary

A Russian speaking actor known as ov1ru$ claimed responsibility for a breach at SyTech, that reportedly took place on July 13. SyTech is a Russian company working on IT projects for the Russian Federal Security Service (FSB). According to ov1ru$, 7.5TB of data were stolen. Hackers posted screenshots of the company's servers on Twitter and shared the stolen data with the DigitalRevolution hacktivist group. DigitalRevolution shared stolen files on their Twitter account, and with Russian journalists. The Russian branch of the BBC[1] was also given access to some documents by the DigitalRevolution group.
The leak reveals at least 20 digital monitoring projects, including:

- "Nautilus": developed between 2009 and 2010 to collect data belonging to social media users on platforms like Facebook, MySpace and LinkedIn. There is no indication about an actual implementation of that project.
- "Nautilus-S": developed in 2012 for the Kvant institute with the objective of de-anonymizing Tor users using rogue exit nodes. Such Russia controlled nodes were discovered in 2014 by researchers from a Swedish university[2]. According to the hackers, this project also allowed the FSB to create active Tor users.
- "Reward": developed between 2013 and 2014 to try to find flaws in the peer-to-peer file sharing protocol BitTorrent. Jabber, OpenFT and ED2K were also analysed.
- "Mentor": developed between by 2013-2014 for Russia's military unit 71330 with the objective to monitor email exchanges.
- "Nadezhda": developed in 2013 and 2014 for Russia's military unit 71330 to monitor the connections between the Internet and RUnet, the Russian domestic segment of internet.
- "Mosquito": commissioned in 2015 to create an infrastructure allowing users to browse the internet anonymously while hiding their interest in the searched information.
- "Tax-3": the most recent of the disclosed projects (2018), allowing the removal from the Federal Tax Service systems of information related to persons placed under protection.

Comments

The DigitalRevolution is a hacktivist group which, in October 2018, promised[3] to punish those who, in their opinion, "turn the Internet into a prison" - the Russian special services, law enforcement agencies and Roskomnadzor, the Russian internet watchdog. Their tactic seems to be the exposure of Russian domestic projects related to online censorship and monitoring.

In November 2018, the DigitalRevolution started to leak Roskomnadzor's internal documents. The same month, they also claimed the compromise of Kvant, a research institute owned by the FSB. It is worth mentioning that, according to WikiLeaks[4] website, Kvant was as a client of the Italian company Hacking Team, which is selling spyware programs.

As regards the SyTech's leak, the BBC Russia said: "it's possible that this is the largest data leak in the history of the work of Russian special services on the Internet." It shows FSB's aims towards extended digital services' surveillance, via different means: spying on communications, social networks usage monitoring, de-anonymization, RUnet control and information gathering.

Several of the non-public projects SyTec performed were for the benefit of military unit 71330. According to the Estonian Foreign Intelligence Service[5], the name "Military Unit 71330" is in fact a front for the FSB's 16th Centre which is FSB's main structural unit for signals intelligence.

1 https://www.bbc.com/russian/features-49050982
2 https://www.cs.kau.se/philwint/spoiled_onions/techreport.pdf
3 https://www.bbc.com/russian/features-46621322
4 https://www.wikileaks.org/hackingteam/emails/?q=kvant&count=50&sort=2
5 https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf