Hackers breach FSB contractor, expose Tor deanonymization project and more

By Written by Catalin Cimpanu, ContributorContributor July 20, 2019 at 5:59 a.m. PT

Archived: 2026-04-05 15:12:35 UTC

See als

Hackers have breached SyTech, a contractor for FSB, Russia's national intelligence service, from where they stole information about internal projects the company was working on behalf of the agency -- including one for deanonymizing Tor traffic.

The breach took place last weekend, on July 13, when a group of hackers going by the name of 0v1ru$ hacked into SyTech's Active Directory server from where they gained access to the company's entire IT network, including a JIRA instance.

Hackers stole 7.5TB of data from the contractor's network, and they defaced the company's website with a "yoba face," an emoji popular with Russian users that stands for "trolling."

Hackers posted screenshots of the company's servers on Twitter and later shared the stolen data with Digital Revolution, another hacking group who last year breached Quantum, another FSB contractor.

This second hacker group shared the stolen files in greater detail on their Twitter account, on Thursday, July 18, and with Russian journalists afterward.


SyTech Digital Revolution

FSB's secret projects

Per the different reports in Russian media, the files indicate that SyTech had worked since 2009 on a multitude of projects since 2009 for FSB unit 71330 and for fellow contractor Quantum. Projects include:

- **Nautilus** - a project for collecting data about social media users (such as Facebook, MySpace, and LinkedIn).
- **Nautilus-S** - a project for deanonymizing Tor traffic with the help of rogue Tor servers.
- **Reward** - a project to covertly penetrate P2P networks, like the one used for torrents.
- **Mentor** - a project to monitor and search email communications on the servers of Russian companies.
- **Hope** - a project to investigate the topology of the Russian internet and how it connects to other countries' network.
- **Tax-3** - a project for the creation of a closed intranet to store the information of highly-sensitive state figures, judges, and local administration officials, separate from the rest of the state's IT networks.

BBC Russia, who received the full trove of documents, claims there were other older projects for researching other network protocols such as Jabber (instant messaging), ED2K (eDonkey), and OpenFT (enterprise file transfer).

Other files posted on the Digital Revolution Twitter account claimed that the FSB was also tracking students and pensioners.

Some projects came to be, were tested

But while most of the projects look to be just research into modern technology -- which all intelligence services carry out -- there are two that appear to have been tested in the real world.

The first was Nautilus-S, the one for deanonymizing Tor traffic. BBC Russia pointed out that work on Nautilus-S started in 2012. Two years later, in 2014, academics from Karlstad University in Sweden, published a paper detailing the use of hostile Tor exit nodes that were attempting to decrypt Tor traffic.

Researchers identified 25 malicious servers, 18 of which were located in Russia, and running Tor version 0.2.2.37, the same one detailed in the leaked files.

The second project is Hope, the one which analyzed the structure and make-up of the Russian segment of the internet.

Earlier this year, Russia ran tests during which it disconnected its national segment from the rest of the internet.

SyTech, the hacked company, has taken down its website since the hack and refused media inquiries.

Photos: Retro computer games that Eastern Europe played as Iron Curtain fell

More data breach coverage:

- Marriott faces $123 million GDPR fine in the UK for last year's data breach
- Hacker steals data of millions of Bulgarians, emails it to local media
- Bulgaria's hacked database is now available on hacking forums
- Hackers breach 62 US colleges by exploiting ERP vulnerability
- Slack resets passwords for 1% of its users because of 2015 hack
- Pale Moon says hackers added malware to older browser versions
- A hacker assault left mobile carriers open to network shutdown **CNET**
- 90% of data breaches in US occur in New York and California **TechRepublic**
