Hackers breach FSB contractor and leak details about IoT hacking project

By Written by Catalin Cimpanu, ContributorContributor March 20, 2020 at 10:23 a.m. PT

Archived: 2026-04-05 16:01:16 UTC

Special feature

Russian hacker group Digital Revolution claims to have breached a contractor for the FSB -- Russia's national intelligence service -- and discovered details about a project intended for hacking Internet of Things (IoT) devices.

The group published this week 12 technical documents, diagrams, and code fragments for a project called "Fronton."

ZDNet has also seen the documents first hand, along with BBC Russia, who first broke the news earlier this week.

Fronton -- the FSB's IoT botnet

According to screenshots shared by the hacker group, which ZDNet asked security researchers to analyze, and based on BBC Russia's report from earlier this week, we believe the Fronton project describes the basics of building an IoT botnet.

The technical Fronton documents were put together following a procurement order placed by one of the FSB's internal departments, unit No. 64829, which is also known as the FSB Information Security Center.

The documents charge InformInvestGroup CJSC, a Russian company with a long history of fulfilling orders for the Russian Ministry of Internal Affairs, with building an IoT hacking tool.

According to the BBC, InformInvestGroup appears to have sub-contracted the project to Moscow-based software company ODT (Oday) LLC, which Digital Revolution claims to have hacked in April 2019.

Based on file timestamps, the project appears to have been put together in 2017 and 2018. The documents heavily reference and take inspiration from Mirai, an IoT malware strain that was used to build a massive IoT botnet in late 2016, which was then used to launch devastating DDoS attacks against a wide range of targets, from ISPs to core internet service providers.

The documents propose building a similar IoT botnet to be made available to the FSB. Per the specs, the Fronton botnet would be able to carry out password dictionary attacks against IoT devices that are still using factory default logins and common username-password combinations. Once a password attack was successful, the device would be enslaved in the botnet.

Fronton targeted IoT cameras and NVRs

Fronton specs say the botnet should specifically target internet security cameras and digital recorders (NVRs), which they deem ideal for carrying out DDoS attacks.

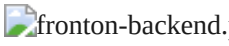
"If they transmit video, they have a sufficiently large communication channel to effectively perform DDoS," the documents read, as cited by BBC Russia.

Around 95% of the entire botnet should be made up of these two types of devices, the documents say, and each infected device should then carry out password attacks against other devices in order to keep the botnet alive.

Furthermore, the botnet should be managed via a web-based administration panel hosted on a command and control (C&C) server, placed behind a network of VPN and proxy servers, in order to hide its real location.


fronton-infra.jpg
Image via Digital Revolution

According to screenshots of the Fronton backend, the botnet was capable of targeting Linux-based smart devices, which account for the vast majority of IoT systems today. This would have allowed it to target more than just smart cameras and NVRs.


fronton-backend.png
Image via Digital Revolution

Per the Fronton specs, the use of the Russian language and the Cyrillic alphabet was strictly forbidden throughout the project and the source code.

The C&C server also needed to be password-protected, and all unused ports should be shut down to prevent other hackers from taking over the botnet's backend infrastructure.

Russian state hackers have a history of hacking IoT devices

The fact that Russian state-backed hackers are interested in acquiring IoT hacking capabilities is no surprise.

In August 2019, Microsoft said that it had observed one of Russia's elite state-sponsored hacking groups breaching IoT devices in order to gain access to a more important target's internal network.

Furthermore, the same group, known as APT28, is also believed to have built and run the VPNFilter IoT botnet, which the FBI took down in 2018. Fronton and VPNFilter appear to be unrelated, according to security researchers who spoke with ZDNet.

Third FSB contractor hack

This week's leaks also mark the third time that Digital Revolution has leaked files from an FSB contractor.

The first victim was a company called Quatum, from where they leaked details in December 2018 about the FSB's social media monitoring projects.

The second was a company called SyTech, from where Ditigal Revolution hackers leaked details about six other FSB projects, ranging from Tor-busting tools to P2P hacking software:

- **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.

The world's most famous and dangerous APT (state-developed) malware

Security
