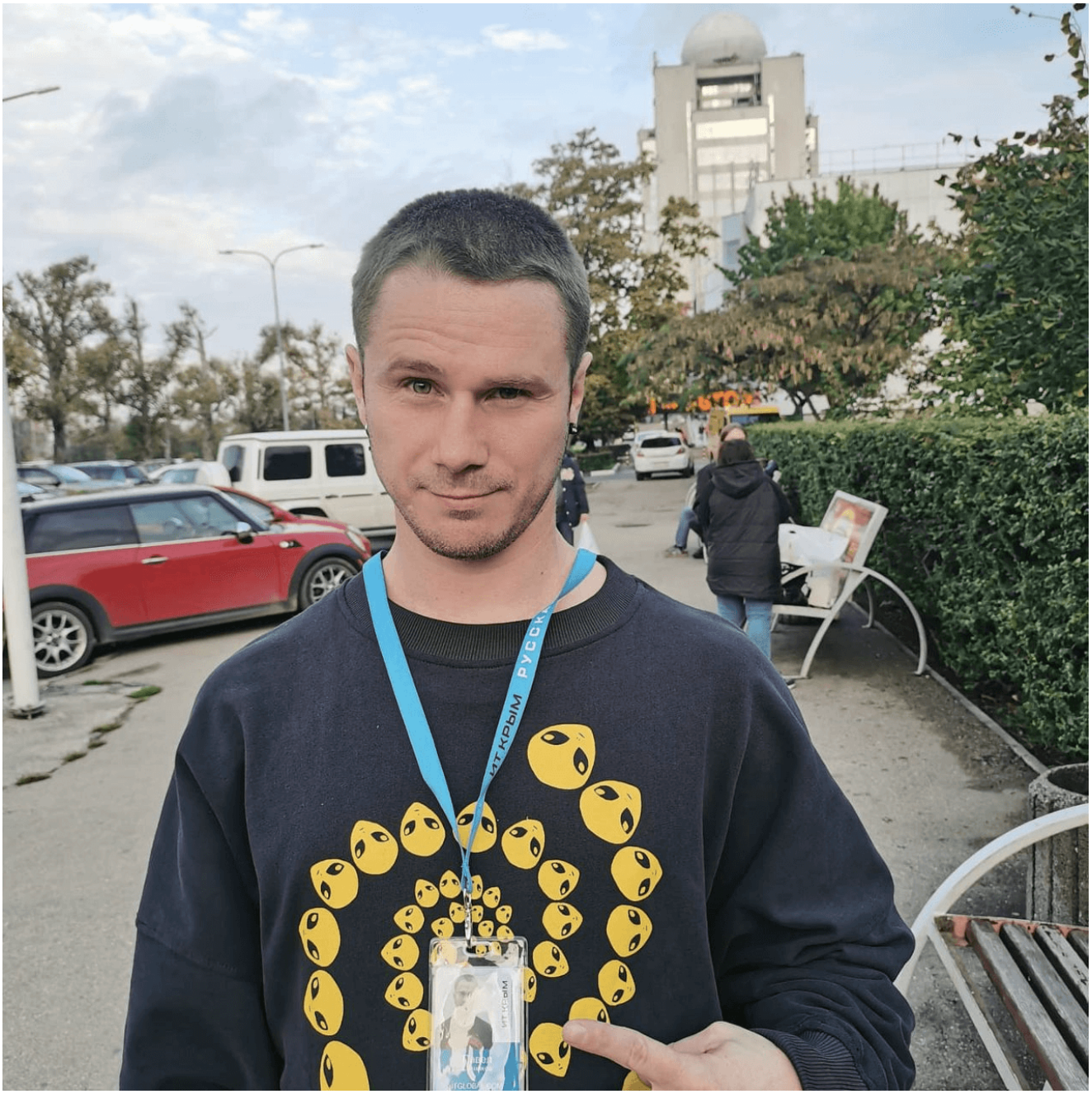
Russian hacker Pavel Sitnikov arrested for sharing malware source code

therecord.media/russian-hacker-pavel-sitnikov-arrested-for-sharing-malware-source-code/

May 31, 2021



Russian authorities have detained earlier this month a popular figure on the Russian hacking scene on charges of distributing malicious software via his Telegram channel.

Pavel Sitnikov, known primarily for operating the now-suspended @Flatl1ne Twitter account and the Freedom F0x Telegram channel, was raided by law enforcement officials on May 20 at his home in the town of Velikiye Luki, in the Pskov region in Eastern Russia.

He was charged the next day under Article 273, Part 2 of Russian criminal law, and forbidden to leave the town or use any electronic devices until his trial.

the main • Documentation • Article 273. Creation, use and distribution of malicious computer programs

"The Criminal Code of the Russian Federation" of 13.06.1996 N 63-FZ (as amended on 05/04/2021, as amended on 08/04/2021)

Criminal Code of the Russian Federation Article 273. Creation, use and distribution of malicious computer programs

(as amended by Federal Law of 07.12.2011 N 420-FZ)
(see text in previous edition)

1. Creation, distribution or use of computer programs or other computer information , deliberately intended for unauthorized destruction , blocking , modification , copying of computer information or neutralization of means of protecting computer information,-

shall be punishable by restraint of liberty for a term of up to four years, or compulsory labor for a term of up to four years, or imprisonment for the same term, with a fine in an amount of up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to eighteen months.

2. Acts provided for in the first part of this Article, committed by a group of persons by prior conspiracy, or by an organized group, or by a person using his official position, as well as causing major damage or committed out of selfish interest,-

shall be punished with restraint of liberty for a term of up to four years, or compulsory labor for a term of up to five years, with or without deprivation of the right to hold certain positions or engage in certain activities for a term of up to three years, or imprisonment for a term of up to five years, with a fine in the amount of one hundred thousand to two hundred thousand rubles, or in the amount of the wages or other income of the convicted person for a period of two to three years or without it and with the deprivation of the right to hold certain positions or engage in certain activities for a period of up to three years or without it.

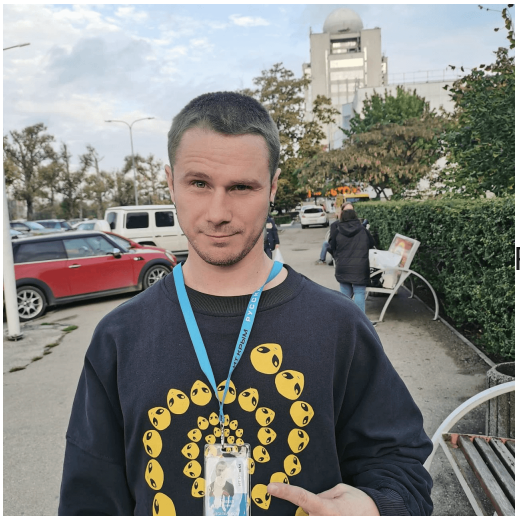
3. The acts provided for in the first or second parts of this Article, if they entailed grave consequences or created a threat of their occurrence,-

the applicable sentence is deprivation of liberty for a term not exceeding seven years.

Sources close to Sitnikov have told Recorded Future analysts that the Russian hacker was allegedly charged for posting the source code of the Anubis banking trojan on Freedom F0x, a Telegram channel where Sitnikov often posted data leaks and malware source code under the pretense of helping the security community.

Suspect's wife claims arrest is payback

But in a video interview with Russian news site Readovka, which first reported on the arrest, Sonia Sitnikov, the suspect's wife, claimed the arrest was actually related to a post her husband made on December 9, last year, when he shared a download link to the personal data of more than 300,000 COVID-19 patients that registered with the Moscow Department of Health.


Pavel Sitnikov

The data, which contained names, phone numbers, addresses, and COVID-19 status, sparked an outcry at the time, but Moscow officials eventually confirmed that the leak occurred because of a human error and not because of a malicious intrusion.

Nevertheless, despite high-ranking officials admitting their mistake, Sitnikov's wife believes the investigation and the Anubis-related charges are payback for publicizing the leak last December.

In an interview with *The Record* last year, Sitnikov touched on the sensitive nature of leaking data from Russian companies, such as banks, and the reason he did it.

> This data is obtained either from the banks themselves, or fraudulently by various cybercriminal groups or researchers. Either sold or leaked publicly. As long as the knowledge about the leak is hidden and not publicized, people affected by the leak continue to suffer. As soon as it is announced, the most important thing is that at least for the moment those who are mentioned in the leak think about their security.
>
> *Pavel Sitnikov*

Suspect faces up to five years in prison

Sitnikov, who at one point claimed to have connections to Russian state-sponsored hacking group APT28 (Fancy Bear), has a long and muddled history on the cybercrime underground.

A member of multiple underground hacking communities, Sitnikov previously sold and shared the source code of multiple malware strains, such as Carberp, Dexter, Alina, Rovnix, and Tinba; hence the reason why the recent charges did not surprise those who followed his past activity.

Under Article 273, Part 2 of Russian criminal law, Sitnikov risks up to five years in prison.

Tags

- Anubis
- arrest
- cybercrime
- data leak
- hacker
- malware
- Russia
- Telegram

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.