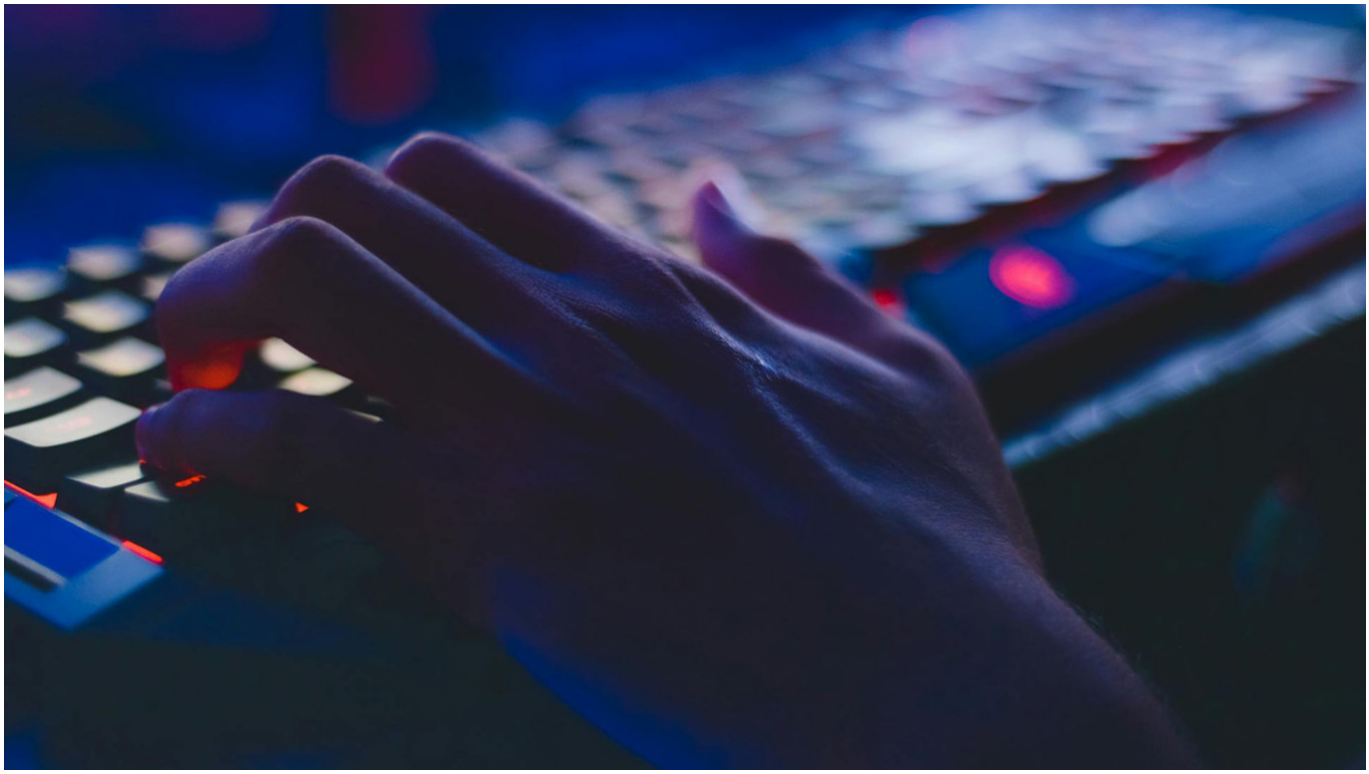
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

FSB-Linked Phishing Campaign Targets Russian Activists, Independent Media

August 14, 2024



Soumil Kumar / pexels

Hackers with suspected connections to Russia's Federal Security Service (FSB) are using sophisticated phishing attacks to target civil society figures in Russia, Europe and the United States, according to a report published by digital rights groups on Wednesday.

The Russian rights organization First Department said that phishing attacks since the start of this year have targeted Russian opposition politicians, human rights activists, NGO workers, media personnel and charities, along with their Belarusian and Western counterparts.

One of the identified attackers is known as Coldriver, a group that the U.S. and British governments previously linked to the FSB's Center for Information Security, also known as Center 18. A second group, called Coldwastrel, was identified by the digital rights nonprofit Access Now.

First Department revealed that it was the "first known target" of Coldwastrel. Access Now suggested that the group "may be acting in the interests of the Russian regime," but said that

it was too early to definitively attribute the attack to a specific entity.

Related article: Moscow Police Arrest U.S. Citizen for Allegedly Assaulting Officer

Citizen Lab, a research group based at the University of Toronto, identified some of the phishing targets, including former U.S. Ambassador to Ukraine Steven Pifer and the independent investigative news outlet Proekt.

However, Citizen Lab noted that "almost all" other targets, many of whom continue to live and work in Russia, have chosen to remain anonymous due to privacy and safety concerns.

"A focus on Russia, Ukraine or Belarus is a common thread running through all of the cases," Citizen Lab said.

First Department described the phishing attacks as involving emails containing encrypted PDF documents sent from addresses impersonating a target's "well-known and reliable colleague." Once the target shared their information, the hackers could gain access to email correspondences and other files on their accounts, and also send new phishing emails to additional targets.

"These attacks could be incredibly harmful, particularly to Russian and Belarusian organizations and independent media, as their email accounts are likely to contain sensitive information about their staff's identities, activities, relationships and whereabouts," Access Now warned.

First Department head Dmitry Zair-Bek told Reuters that "some" of the phishing attack targets had "fallen for it."

Russian officials have not commented on the report, though Moscow has consistently denied involvement in previous cyber-espionage campaigns.

Original url:
https://www.themoscowtimes.com/2024/08/14/fsb-linked-phishing-campaign-targets-russian-activists-independent-media-a86020