FSB NKTsKI: Foreign ‘cyber mercenaries’ breached Russian federal agencies

therecord.media/fsb-nktski-foreign-cyber-mercenaries-breached-russian-federal-agencies/

May 21, 2021

Foreign hackers have breached and stolen information from Russian federal executive bodies, the Russian government said in a report published last week.

The attacks were identified in 2020.

They were detailed in a joint report authored by Rostelecom-Solar, a cybersecurity division of Russian telecom giant Rostelecom, and the National Coordination Center for Computer Incidents (NKTsKI), a CERT-like organization created by the Russian Federal Security Service (FSB) in 2018.

“Evaluating attackers in terms of training and qualifications (used technologies and mechanisms, the speed and quality of the work done by them), we are inclined to classify this group as **cyber mercenaries pursuing the interests of a foreign state**,” the report reads.

Attackers used novel malware

To breach Russian federal agencies, Rostelecom and NKTsKI said the attackers used a broad set of entry vectors that included spear-phishing, exploiting vulnerabilities in web applications, and hacking the IT infrastructure of government contractors.

“After a complete compromise of the infrastructure, the attackers proceeded to collect confidential information from all sources of interest: such as mail servers, electronic document management servers, file servers, and workstations of various levels,” the report said.

Once they breached a victim, the attackers would deploy two never-before-seen malware strains named **Mail-O** and **Webdav-O**, both stealthy backdoors that the intruders used to execute commands on infected hosts and steal data.

Both strains exfiltrated data to command and control infrastructure hosted on local Russian cloud providers, with Mail-O uploading data to Mail.ru Cloud servers and Webdav-O to the Yandex.Disk cloud.

Both Mail-O and Webdav-O were also designed to bypass Kaspersky antivirus software, which is usually installed on Russian federal networks, and disguised their network traffic as legitimate communications for Mail.ru’s Disk-O and the Yandex.Disk applications.

The joint report contains additional technical details about the inner workings of both malware strains.

Russian authorities did not attribute the attack to any specific country as of yet.

The report comes a month after the US government formally attributed the SolarWinds supply-chain attack to a cyber-espionage operation carried out by the Russian Foreign Intelligence Service.

Tags

- APT
- FSB
- Mail.ru
- nation-state
- NKTsKI
- Russia
- Yandex

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.