# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:02:49 UTC



## APT group: CloudSorcerer

| | | |
|---|---|---|
| Names | CloudSorcerer *(Kaspersky)* | |
| Country | [Unknown] | |
| Motivation | Information theft and espionage | |
| First seen | 2024 | |
| Description | (Kaspersky) In May 2024, we discovered a new advanced persistent threat (APT) targeting Russian government entities that we dubbed CloudSorcerer. It's a sophisticated cyberespionage tool used for stealth monitoring, data collection, and exfiltration via Microsoft Graph, Yandex Cloud, and Dropbox cloud infrastructure. The malware leverages cloud resources as its command and control (C2) servers, accessing them through APIs using authentication tokens. Additionally, CloudSorcerer uses GitHub as its initial C2 server.<br><br>CloudSorcerer's modus operandi is reminiscent of the CloudWizard APT (Bad Magic, RedStinger) that we reported on in 2023. However, the malware code is completely different. We presume that CloudSorcerer is a new actor that has adopted a similar method of interacting with public cloud services. | |
| Observed | Sectors: Government.<br>Countries: Russia. | |
| Tools used | GrewApacha, PlugY, The CloudSorcerer. | |
| Operations performed | Jul 2024 | Operation "EastWind"<br>EastWind campaign: new CloudSorcerer attacks on government organizations in Russia<br><https://securelist.com/eastwind-apt-campaign/113345/> |
| Information | <https://securelist.com/cloudsorcerer-new-apt-cloud-actor/113056/> | |

Last change to this card: 27 August 2024

Download this actor card in PDF or JSON format

---