# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:43:57 UTC

Home > List all groups > Cadet Blizzard

## APT group: Cadet Blizzard

| | |
|---|---|
| Names | Cadet Blizzard *(Microsoft)*<br>DEV-0586 *(Microsoft)*<br>Ruinous Ursa *(Palo Alto)* |
| Country | Russia |
| Sponsor | State-sponsored, GRU |
| Motivation | Information theft and espionage, Sabotage and destruction |
| First seen | 2020 |
| Description | (Microsoft) Microsoft assesses that Cadet Blizzard operations are associated with the Russian General Staff Main Intelligence Directorate (GRU) but are separate from other known and more established GRU-affiliated groups such as Forest Blizzard (Sofacy, APT 28, Fancy Bear, Sednit) and Seashell Blizzard (Sandworm Team, Iron Viking, Voodoo Bear). While Microsoft constantly tracks a number of activity groups with varying degrees of Russian government affiliation, the emergence of a novel GRU affiliated actor, particularly one which has conducted destructive cyber operations likely supporting broader military objectives in Ukraine, is a notable development in the Russian cyber threat landscape. A month before Russia invaded Ukraine, Cadet Blizzard foreshadowed future destructive activity when it created and deployed WhisperGate, a destructive capability that wipes Master Boot Records (MBRs), against Ukrainian government organizations. Cadet Blizzard is also linked to the defacements of several Ukrainian organization websites, as well as multiple operations, including the hack-and-leak forum known as “Free Civilian”.<br><br>Microsoft has tracked Cadet Blizzard since the deployment of WhisperGate in January 2022. We assess that they have been operational in some capacity since at least 2020 and continue to perform network operations through the present. Operationally consistent with the remit and assessed objectives of GRU-led operations throughout Russia’s invasion of Ukraine, Cadet Blizzard has engaged in focused destructive attacks, espionage, and information operations in regionally significant areas. Cadet Blizzard’s operations, though comparatively less prolific in both scale and scope to more established threat actors such as Seashell Blizzard, are |

| | | |
|---|---|---|
| | structured to deliver impact and frequently run the risk of hampering continuity of network operations and exposing sensitive information through targeted hack-and-leak operations. Primary targeted sectors include government organizations and information technology providers in Ukraine, although organizations in Europe and Latin America have also been targeted. | |
| Observed | Sectors: Government, IT, Law enforcement, NGOs.<br>Countries: Ukraine and Europe, Central Asia and Latin America. | |
| Tools used | GO Simple Tunnel, Impacket, netcat, P0wnyshell, reGeorg, WhisperGate, Living off the Land. | |
| Operations performed | Jan 2022 | Operation “Bleeding Bear”<br>Destructive malware targeting Ukrainian organizations<br><https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/> |
| Counter operations | Jun 2024 | Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data<br><https://www.justice.gov/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian> |
| Information | <https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/> | |
| Playbook | <https://pan-unit42.github.io/playbook_viewer/?pb=ruinousursa> | |

Last change to this card: 26 August 2024

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=4f64a76f-0650-49dd-9386-d7813916463a