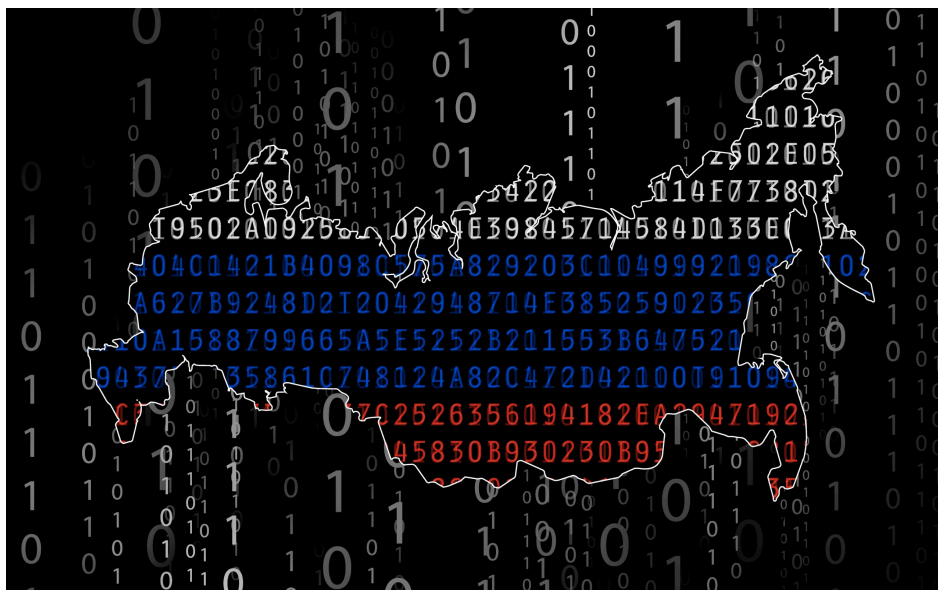


Ongoing Russian cyberattacks targeting Ukraine

[Topics](#)
[Cloud Principles](#)
[Press Tools](#)

Jun 14, 2023 | [Tom Burt - Corporate Vice President, Customer Security & Trust](#)



Microsoft threat intelligence teams have been tracking a wave of cyberattacks from an actor we call Cadet Blizzard that is associated with the Russian GRU. These attacks, which began in February 2023, targeted government agencies and IT service providers in Ukraine. We can also now attribute to Cadet Blizzard the destructive WhisperGate wiper attacks against Ukraine [detected by Microsoft](#) in January 2022 prior to Russia's invasion.

Cadet Blizzard typically breaches its targets by using stolen credentials to gain access to internet servers that sit on the perimeters of an organization's network. Once inside, it seeks to maintain access by using broadly available tools called web shells, which can be bought as off-the-shelf kits and customized. It then uses "living off the land" techniques – that is, it commonly uses legitimate commands, not malware, to move laterally across its targets' networks while gaining access to more information or disrupting networks if it chooses. The

May 2, 2023 | [Clint Watts](#)

Rinse and repeat: Iran accelerates its cyber influence operations worldwide >

Apr 19, 2023 | [Kate Behncken](#)

The world needs cybersecurity experts – Microsoft expands skilling effort with a focus on women >

Apr 11, 2023 | [Amy Hogan-Burney](#)

Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries >

Related Blogs

May 25, 2023 | [Brad Smith](#)

use of “living off the land” techniques help it hide in legitimate network traffic, making its activities harder to detect.

Cadet Blizzard is active seven days a week and has conducted its operations during its primary targets’ off-business hours when its activity is less likely to be detected. In addition to Ukraine, it also focuses on NATO member states involved in providing military aid to Ukraine.

What’s perhaps most interesting about this actor is its relatively low success rate compared with other GRU-affiliated actors like Seashell Blizzard (Iridium) and Forrest Blizzard (Strontium). The February 2022 wiper attacks attributed to Seashell Blizzard alone affected more than 200 systems spanning over 15 organizations, while Cadet Blizzard’s January 2022 WhisperGate attack affected an order of magnitude fewer systems and delivered comparatively modest impact, despite being trained to destroy the networks of their opponents in Ukraine. Cadet Blizzard’s activity spiked between January and June of 2022, dissipated, and re-emerged in early 2023. The more recent Cadet Blizzard cyber operations, although occasionally successful, similarly failed to achieve the impact of those conducted by its GRU counterparts.

The group’s influence operations work has also gained modest results. In early 2022, it successfully defaced a number of Ukrainian websites. However, the “Free Civilian” Telegram channel, which Cadet Blizzard uses to distribute information it obtains from hack-and-leak operations, had only 1.3K followers as of February 2023, with posts gaining at most a dozen reactions as of the time of publication, signifying low user interaction.

We believe Cadet Blizzard has been operating since 2020. In addition to Ukraine and NATO member states, it has targeted a range of organizations in Europe and Latin America.

While it has not been the most successful Russian actor, Cadet Blizzard has seen some recent success. Microsoft’s unique visibility into their operations has motivated us to share information with the security ecosystem and customers to raise visibility and protections against their attacks. As we always do, we’ve notified customers who have been targeted or breached and, today, shared [detailed technical information](#) to help the security community identify and defend against this actor’s attacks.

How do we best govern AI? >

May 18, 2023 | [Jenny Lay-Flurrie](#)

Global Accessibility Awareness Day – Accessibility at the heart of innovation >

May 16, 2023 | [Vickie Robinson](#)

Microsoft Airband will expand internet access to nearly 40 million people across Latin America and Africa >

More Cybersecurity Stories

Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries >

April 11, 2023

Tags: [cyber influence](#), [cyberattacks](#), [Digital Threat Analysis Center](#), [digital threats](#), [Ukraine](#)

Digital Crimes Unit:
Leading the fight
against cybercrime >

May 3, 2022

Keeping your vote
safe and secure: A
story from inside the
2020 election >

June 22, 2021

Follow us: 

What's new

Surface Laptop
Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft
products

Windows 11 apps

Microsoft
Store

Account profile

Download Center

Microsoft Store
support

Returns

Order tracking

Certified
Refurbished

Microsoft Store
Promise

Flexible Payments

Education

Microsoft in
education

Devices for
education

Microsoft Teams
for Education

Microsoft 365
Education

How to buy for
your school

Educator training
and development

Deals for
students and
parents

Azure for
students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power
Platform

Microsoft Teams

Copilot for
Microsoft 365

Small Business

Developer &
IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech
Community

Azure
Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at
Microsoft

Investors

Diversity and
inclusion

Accessibility

Sustainability



English (United States)



Your Privacy Choices

Consumer Health Privacy

Contact us

Privacy

Terms of use

Trademarks

About our ads

© Microsoft 2024