

HiveForce Labs

# THREAT ADVISORY



## ATTACK REPORT

### Unveiling Cadet Blizzard APT's Wiper Attacks Targeting Ukraine

Date of Publication

June 15, 2023

Last Updated Date

June 19, 2023

Admiralty Code

A2

TA Number

TA2023265

# Summary

**First appeared:** January 2022

**Actor Name:** Cadet Blizzard (aka DEV-0586, Ruinous Ursa)

**Malware:** WhisperGate

**Attack Region:** Europe, Central Asia, and Latin America

**Targeted Sectors:** Government services, Law enforcement, Non-profit/non-governmental organizations, IT service providers/consulting, and Emergency services.










**Attack:** Cadet Blizzard, a Russian GRU-sponsored threat group, conducted major cyber operations using WhisperGate, a customized wiper malware, to demonstrate their destructive capabilities through targeted attacks on Ukrainian government organizations.

## 🗺️ Attack Regions



## ⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-26084	Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	Atlassian Confluence Server and Data Center	❌	✅	✅
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon	❌	✅	✅
CVE-2021-4034	Red Hat Polkit Out-of-Bounds Read and Write Vulnerability	Red Hat Polkit	❌	✅	✅

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability (Proxyshell)	Microsoft Exchange Server			
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability (Proxyshell)	Microsoft Exchange Server			
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability (Proxyshell)	Microsoft Exchange Server			

# Attack Details

## #1

Cadet Blizzard is a threat group sponsored by the Russian GRU. In January 2022, Cadet Blizzard demonstrated its potential for future destructive actions by utilizing a customized wiper malware called WhisperGate. This capability targets Master Boot Records (MBRs) and was deployed against Ukrainian government organizations.

## #2

Cadet Blizzard typically infiltrates and maintains control over compromised networks for months, often stealing data before carrying out disruptive activities. The group's peak activity was observed between January and June 2022, followed by a period of reduced operations. However, Cadet Blizzard resurfaced in January 2023 with increased attacks on multiple entities in Ukraine and Europe, including a new series of website defacements.

## #3

Cadet Blizzard typically gains initial access by exploiting web servers commonly found on network perimeters and DMZs. The group has also been identified for exploiting Confluence servers through the CVE-2021-26084 vulnerability, and Exchange servers through multiple vulnerabilities, including CVE-2022-41040 and proxyshell.

## #4

Additionally, they may potentially utilize commodity vulnerabilities in various open-source platforms, such as content management systems. Cadet Blizzard follows traditional network operator practices, often employing living-off-the-land strategies to navigate across the network, acquire passwords and other sensitive information, and implement defense evasion techniques and persistence mechanisms following their initial access.

# Recommendations



**Strengthen Web Server Security:** Enhance the security of web servers located on network perimeters and DMZs to mitigate the risk of initial access by threat actors like Cadet Blizzard. Regularly patch and update server software and employ strong access controls and authentication mechanisms.



**Prioritize Patching:** Ensure timely patching of known vulnerabilities in frequently targeted systems, including Confluence servers, Exchange servers, and open-source platforms. Promptly apply security updates and **fixes** provided by vendors to address vulnerabilities such as CVE-2021-26084 (update to version 6.13.23, 7.4.11, 7.11.6, 7.12.5 or later), CVE-2022-41040, and proxyshell others.



**Implement Robust Network Defense:** Deploy comprehensive network defense measures, including intrusion detection and prevention systems, network segmentation, and behavior-based monitoring. Focus on detecting and mitigating lateral movement attempts, password theft, defense evasion techniques, and persistence mechanisms employed by threat actors like Cadet Blizzard. Regular security assessments and threat intelligence sharing can enhance preparedness against evolving cyber threats.

## Potential MITRE ATT&CK TTPs

<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0005</u></b> Defense Evasion
<b><u>TA0006</u></b> Credential Access	<b><u>TA0009</u></b> Collection	<b><u>TA0011</u></b> Command and Control	<b><u>TA0040</u></b> Impact
<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1059.001</u></b> PowerShell	<b><u>T1059.005</u></b> Visual Basic	<b><u>T1055</u></b> Process Injection
<b><u>T1055.012</u></b> Process Hollowing	<b><u>T1562</u></b> Impair Defenses	<b><u>T1562.001</u></b> Disable or Modify Tools	<b><u>T1132</u></b> Data Encoding
<b><u>T1132.001</u></b> Standard Encoding	<b><u>T1102</u></b> Web Service	<b><u>T1071</u></b> Application Layer Protocol	<b><u>T1071.001</u></b> Web Protocols
<b><u>T1105</u></b> Ingress Tool Transfer	<b><u>T1561</u></b> Disk Wipe	<b><u>T1561.002</u></b> Disk Structure Wipe	<b><u>T1486</u></b> Data Encrypted for Impact

## ⌘ Indicators of Compromise (IOCs)

TYPE	VALUE
<b>Domain</b>	justiceua[.]org
<b>IPV4</b>	179.43.187[.]33
<b>MD5</b>	3a2a2de20daa74d8f6921230416ed4e6
<b>SHA256</b>	3e4bb8089657fef9b8e84d9e17fd0d7740853c4c0487081dacc4f22359bade5c 20215acd064c02e5aa6ae3996b53f5313c3f13625a63da1d3795c992ea730191 3fe9214b33ead5c7d1f80af469593638b9e1e5f5730a7d3ba2f96b6b555514d4 23d6611a730bed886cc3b4ce6780a7b5439b01ddf6706ba120ed3eb3b1c478 7fedaf0dec060e40cbdf4ec6d0fbfc427593ad5503ad0abaf6b943405863c897

## ⌘ Patch Links

<https://jira.atlassian.com/browse/CONFSERVER-67940>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472>

[https://bugzilla.redhat.com/show\\_bug.cgi?id=2025869](https://bugzilla.redhat.com/show_bug.cgi?id=2025869)

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207>

## ⌘ References

<https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/>

<https://www.hivepro.com/ukraine-government-entities-targeted-by-a-destructive-malware-whispergate/>

<https://unit42.paloaltonetworks.com/atoms/ruinousursa/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**June 15, 2023 • 6:03 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)