

APT Profile: Cozy Bear / APT29

March 17, 2023

[Update] November 16, 2023: See the subheading: "APT29 Exploits WinRAR Vulnerability (CVE-2023-38831) in European Embassy Attacks."

[Update] August 3, 2023: Microsoft identified a new wave of social engineering attacks by APT29. See the subheading: "APT29's New Phishing Lures Involve Microsoft Teams Chats."


[Update] April 14, 2023: Poland's Military Counterintelligence Service and CERT have linked APT29 to ongoing and developing attacks against NATO and European Union countries. APT29 collects information from diplomatic entities and foreign ministries through spear-phishing emails and infected websites. The websites infect users with the EnvyScout dropper using HTML smuggling. The dropper installs the SNOWYAMBER and QUARTERRIG downloaders and the HALFRIG CobaltStrike Beacon stager.

Advanced Persistent Threat (APT) groups are widely classified as organizations that lead "attacks on a country's information assets of national security or strategic economic importance through either cyber espionage or cyber sabotage." They are elusive, eminent, and influential at what they do: wreaking havoc on their targets. The Cozy Bear group is one of them. In today's blog post, we'll learn more about that group and what this group has done.

A Russian Hacking Organization: Cozy Bear

Cozy Bear is a Russian hacker group allegedly affiliated with one or more Russian intelligence agencies. Mandiant identifies this group as the advanced persistent threat APT29. The group has the advanced capabilities to launch highly targeted attacks like **SolarWinds** supply-chain attacks where trojanized software updates have been used to infect the MSSP customers.

The Dutch General Intelligence and Security Service (AIVD) inferred from security camera footage that it is led by the Russian Foreign Intelligence Service (SVR); the US agrees. CrowdStrike, a cybersecurity firm, previously speculated that the group might be linked to the Russian Federal Security Service (FSB). CozyCar, CozyDuke (by F-Secure), Dark Halo, The Dukes (by Volexity), NOBELIUM, Office Monkeys, StellarParticle, UNC2452, and YTTIRIUM are some of the nicknames given to the group by different cybersecurity research groups.



Last Modified: 25 October 2021

APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. [1] [2] This group reportedly compromised the Democratic National Committee starting in the summer of 2015. [3]

Target Countries:

Belgium

Brazil

China

Georgia

India

Japan

Kazakhstan

Mexico

New Zealand

Portugal

Romania

South Korea

Turkey

Ukraine

United States

Sectors:

Government

Private sector

Aliases:

Dukes

Group 100

Cozy Duke

CozyDuke

EuroAPT

CozyBear

CozyCar

Cozer

Office Monkeys

OfficeMonkeys

APT29

Cozy Bear

The Dukes

Minidionis

SeaDuke

Hammer Toss

YTTIRIUM

Iron Hemlock

Grizzly Steppe

APT29 Profile Card from SOCRadar [Cyber Threat Intelligence](#)

Cozy Bear is a well-resourced, highly dedicated, and structured cyberespionage operation that we believe has been operating for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making,' according to a 2015 assessment from F-Secure. Cozy Bear has an unusual amount of faith in its ability to keep effectively compromising its targets, as well as in its ability to operate without being detected.

Cyber Attacks Associated with APT29

APT29 and another Russian APT group called **APT28 (Fancy Bear)** infiltrated the Democratic National Committee's (DNC) network and caused a data breach, which started in 2015 but was detected in 2016.

ESET investigates **Operation Ghost**, which is believed to have started in 2013 and affected the Ministry of Foreign Affairs of some European countries. ESET also reports that the group has developed new malware families called the **PolyglotDuke, RegDuke, and FatDuke**.

Later on, the **WellMess malware** was observed in attacks against Japanese firms in 2018; however, it was not linked to a specific threat actor then. WellMess was linked to Russia's **APT29** in 2020 when the US, UK, and Canada stated Russian hackers used it in attacks against academic and pharmaceutical research institutes involved in developing the COVID-19 vaccine.

APT29, who are the hackers behind the SolarWinds software supply chain attack and the attacks mentioned above, have continued to look for ways to access enterprise networks by targeting IT and cloud services providers with admin rights on their customers' systems due to their business connection. In a new report, Microsoft warns that the gang has targeted over 140 cloud service resellers and technology suppliers since May and has succeeded in compromising as many as 14. Moreover, Cozy Bear is the hacker behind the SolarWinds software supply chain attack.

Denmark National Bank has been another victim of the notorious group's SolarWinds attack. According to a report published in May 2021, Cozy Bear attacked Denmark's central bank (Denmark's National Bank) and planted malware that allowed them to access the network for over six months without being noticed.

The SolarWinds campaign is regarded as one of the most sophisticated supply-chain hacks, with 18,000 businesses worldwide downloading trojanized versions of the IT management platform SolarWinds Orion. Despite the hackers' long-term access, the bank said it found no sign of breach beyond the first stage of the attack, as thousands of other companies did when they installed the trojanized version of SolarWinds Orion.

[REQUEST DEMO](#)
[FREE ACCESS](#)
[FREE TOOLS](#)

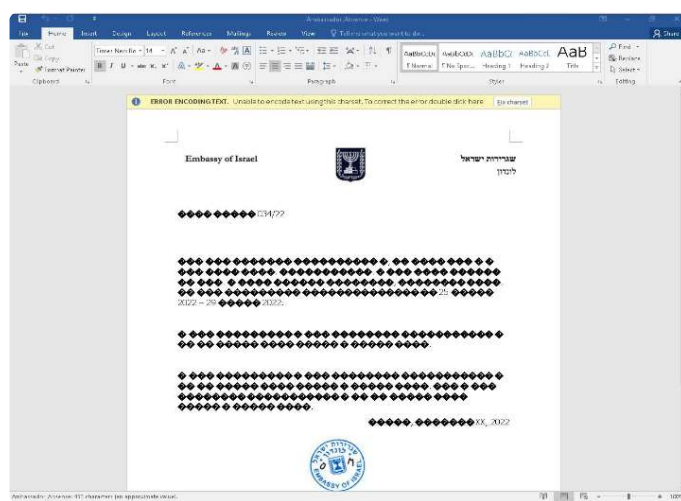


Attributed attacks to the Russian-speaking hack group Cozy Bear on [DarkMirror](#)

In a [blog](#) shared by Microsoft Threat Intelligence Center (MSTIC) in 2021, researchers noted that APT29 has been using the [EnvyScout](#), [BoomBox](#), [NativeZone](#), and [VaporRage](#) malware families for its email-based attacks since February 2021, which aims to gain a foothold on various sensitive diplomatic and government entities.

In December 2021, ANSSI shared a threat and incident [report](#) of the French national government computer security incident response team (CERTFR). The ANSSI stated that French organizations had been subjected to [phishing attacks](#) since February 2021, and the identified TTPs overlapped with the [SolarWinds supply chain attack](#).

In April 2022, a lure document that allegedly belonged to APT29 was found, which contained a malicious script and appeared to have been created by the [Israeli Embassy](#).



Malicious lure document allegedly used in APT29 campaign (Source: [Inquest](#))

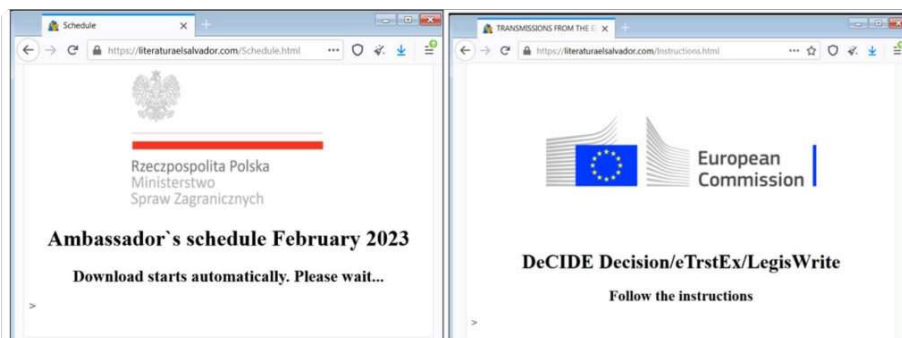
In January 2022, Crowdstrike shared a [blog](#) about a campaign called [StellarParticle](#) linked to Cozy Bear. The campaign, conducted with [GoldMax](#) and [TrailBlazer](#) malware, reveals that since mid-2019, APT29 has used an [MFA bypass](#) to access [Office 365](#) accounts with stolen cookies.

Cybersecurity researchers observed that the group uses social media platforms ([Twitter](#), [Reddit](#), etc.) or various internet services ([Trello](#), [Firebase](#), etc.) as [C2](#) ([Command & Control](#)) communication during its activities.

In the group's latest campaign, it was found that they have been using the API of [Notion](#), a note-taking application. Based on the group's latest campaign details, APT29 used the [Polish Foreign Minister's](#) recent visit to the US as a lure to conduct a [spear phishing](#) campaign targeting Western Countries, particularly Western Europe.

The lure document contains a [link](#) to download an [HTML file](#) from a legitimate online library the group had actively used in its other attacks between January 2023 to February 2023.

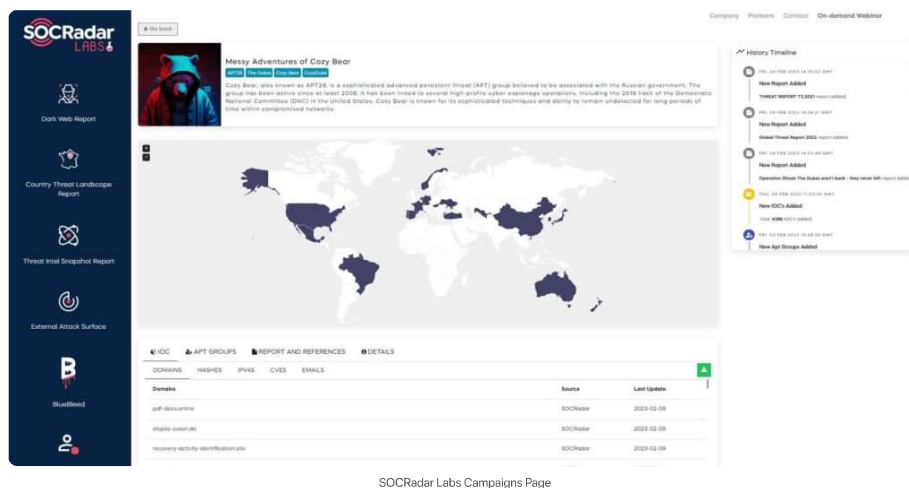
Another observed lure document abuses multiple legitimate systems, such as [LegisWrite](#) and [eTrustEx](#), which EU nations use to exchange information and transfer data securely. Using these programs shows that the group targets state organizations within the EU.



Lure documents used in the latest phishing campaign of APT29 (Source: [Blackberry](#))

You can follow the updates about the latest campaigns of APT29 from the [Messy Adventures of Cozy Bear campaign page](#) in SOCRadar LABS.

REQUEST DEMO
FREE ACCESS
FREE TOOLS



SOCRadar Labs Campaigns Page

APT29's New Phishing Lures Involve Microsoft Teams Chats

Microsoft Threat Intelligence has identified **highly targeted social engineering attacks**, in which APT29 (tracked as Midnight Blizzard by Microsoft), sent phishing lures as Microsoft Teams chats. The threat actor has been posing as tech support staff in Microsoft Teams chats to steal **login credentials** from numerous global organizations.

To execute their schemes, the hackers used **compromised Microsoft 365 accounts** belonging to small businesses to create **new domains** that appeared to be legitimate technical support entities, cleverly incorporating the word **"microsoft"** in them.

The researchers further disclosed that the hackers targeted a range of sectors, including government, non-government organizations (NGOs), IT services, technology, discrete manufacturing, and media. Approximately **40** global organizations fell victim to these attacks, with Microsoft still actively investigating the incidents that started **in late May**.

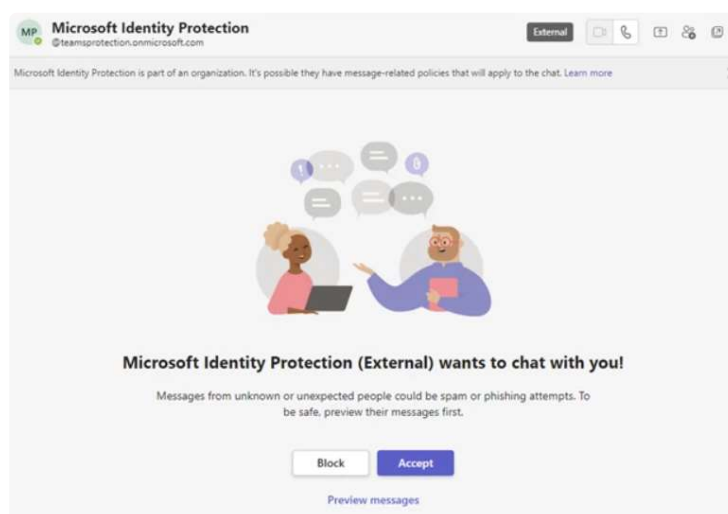
Microsoft was able to mitigate the issue by preventing the attackers from using these domains and continues to investigate the activity. According to the researchers, this recent attack, along with their previous activities, showcases Midnight Blizzard's persistent use of both new and common techniques to achieve their objectives.

Microsoft has previously linked a surge in credential theft attacks to Midnight Blizzard (APT29), identifying the threat actor as a significant concern. For further details, refer to our recent blog post:

[Credential Theft Attacks Surge: Microsoft Raises Red Flag on Midnight Blizzard \(APT29\)](#)

The Phishing Attack Chain

The threat actor, masquerading as **technical support** or **security team**, initiates the attack by sending a Microsoft Teams message request to the target user.



Message request by the APT29 threat actor

If the target user accepts the request, the attacker will attempt to convince them to enter a code into the Microsoft **Authenticator app** on their mobile device.

If the targeted user falls for this and enters the code, the threat actor gains a **token** that allows them to authenticate as the target user. Consequently, the attacker successfully infiltrates the user's Microsoft 365 account and proceeds with post-compromise activities. These activities typically involve the **theft of information** from the compromised Microsoft 365 tenant.

Furthermore, the attacker **may attempt to add a device** to the organization using Microsoft Entra ID (**formerly Azure Active Directory**). This action is likely an attempt to bypass conditional access policies set up to restrict access to specific resources solely to managed devices.

Indicators of Compromise (IoCs):

- msftprotection.onmicrosoft[.]com
- identityVerification.onmicrosoft[.]com
- accountsVerification.onmicrosoft[.]com
- azuresecuritycenter.onmicrosoft[.]com
- teamsprotection.onmicrosoft[.]com

For more information regarding these attacks, visit Microsoft's [security blog](#).

REQUEST DEMO
FREE ACCESS
FREE TOOLS

APT29 Exploits WinRAR Vulnerability (CVE-2023-38831) in European Embassy Attacks

The National Security and Defense Council of Ukraine has detailed APT29 attacks on European embassies, exploiting the WinRAR vulnerability (CVE-2023-38831). The campaign, which started in September 2023, targeted diplomatic entities in Azerbaijan, Greece, Romania, and Italy.

Known targeted organizations are listed as follows:

Domain	Organization
@gccsg.org	Secretariat General of the Gulf Cooperation Council
@ec.europa.eu	European Commission
@unhcr.org	United Nations High Commissioner for Refugees
@unicef.org	United Nations International Children's Emergency Fund
@auf.org	Agence universitaire de la Francophonie
@francophonie.org	Organisation Internationale de la Francophonie (OIF)
@iom.int	International Organization for Migration
@worldbank.org	The World Bank
@selec.org	Southeast European Law Enforcement Center
@coe.int	Council of Europe
@euro.who.int	World Health Organization European Region

Organizations targeted by APT29 in attacks exploiting CVE-2023-38831 (The National Security and Defense Council of Ukraine)

APT29 used BMW car sale-themed lures with a RAR archive (DIPLOMATIC-CAR-FOR-SALE-BMW.rar) to deliver malware through compromised PDFs, exploiting the WinRAR vulnerability to gain entry to compromised systems.

You can learn more about the WinRAR vulnerability, CVE-2023-38831, by visiting [our other blog post](#).

The report underscores the geopolitical implications of the campaign, suggesting that Russia's Foreign Intelligence Service (SVR) aims to gather intelligence on Azerbaijan's strategic activities, particularly in the context of the Azerbaijani invasion of Nagorno-Karabakh. The targeted countries – Azerbaijan, Greece, Romania, and Italy – have significant political and economic ties with Azerbaijan, while the report also reminds of a recent arms deal with Italy for military aircraft.

APT29's use of the WinRAR vulnerability (CVE-2023-38831) and their adoption of Ngrok services for covert communications are highlighted in the report. APT29 employed Ngrok, a tool designed to securely expose local network ports to the internet by tunnelling, for storing and communicating with malicious payloads. This adaptation allows adversaries to obfuscate their activities, complicate cybersecurity efforts, and evade detection.

For more information and Indicators of Compromise (IOCs) related to this campaign, refer to the [full report](#).

Malware Used by APT29 / Cozy Bear

The malware used by APT29 could be tailored to the victim's IT environment by the attackers. Cozy Bear malware's backdoor components are upgraded over time with cryptography, trojan functionality, and anti-detection changes. The rapidity with which Cozy Bear builds and distributes its components is reminiscent of Fancy Bear's (APT28) toolkit, including CHOPSTICK and CORESHELL.

Also, some of the malware that APT29 has been observed to use are listed in the table below:

HAMMERTOSS	SeaDuke	FatDuke	CozyCar
CosmicDuke	SeaDaddy	PolyglotDuke	PinchDuke
WellMess	RegDuke	MiniDuke	OnionDuke
SUNBURST	POSHSPY	Boombox	SoreFang

REQUEST DEMO

FREE ACCESS

FREE TOOLS

Critical Vulnerabilities Exploited by APT29 to Gain Initial Foothold

APT29 and its activities are closely monitored by The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). In April 2021, CISA released a vital advisory on the [critical vulnerabilities](#) exploited by APT29.

The vulnerabilities exploited by the APT29 are listed below:

- CVE-2018-13379 – Fortinet FortiOS
- CVE-2019-9670 – Zimbra Collaboration Suite
- CVE-2019-11510 – Pulse Secure VPN Appliance
- CVE-2019-19781 – Citrix ADC Network Gateway
- CVE-2020-4006 – VMware Workspace ONE Access
- CVE-2022-30170 – Windows Credential Roaming Service Elevation of Privilege Vulnerability.

Defending Against APT Groups

Patch management and other strategies can assist in the defense against APT29 and other similar threats:

- Increase your efforts to identify digital shadow assets, including the cloud hosts, by using an [Attack Surface Management](#) solution
- Keep the internet-facing technologies and appliances patched at all times since threat actors continuously scan to detect these blind spots.
- Be wary of external remote services like [RDP](#), which is known to be vulnerable. If not necessary, close it down.
- Quickly take action when you're alerted by your Threat Intelligence or [Digital Risk Protection](#) platform about compromised employee credentials.
- Continuously check for potential weaknesses on your internet infrastructure like expired domains, [SSL certificates](#), or subdomains.
- Keep the password hygiene within the organization at peak condition at all times.
- Make sure [EDR](#) and logging functions are in place to detect suspicious actions within the network. It is only one component of the protection plan.



Share this:   

Latest Posts



Digital Predators of 2023: Exposing Top Cyber Threat Actors



Dark Web Sales: A New RCE Exploit, US Credit Cards, and 19M Japanese Emails



Latest Critical Vulnerabilities Affecting GitLab, Apple's Magic Keyboard, and Juniper Networks' Junos OS



CISA Issues ICS Advisories for Vulnerabilities Affecting Siemens, Schneider Electric, Rapid Software, Horner Automation



Beyond H KillNet, ar

SOCRadar

- Home
- Cyber Threat Intelligence
- Digital Risk Protection
- External Attack Surface Management
- SOCRadar Labs
- Free Access

Use Cases

- Credential & Data Leak Detection
- Dark & Deep Web Monitoring
- Phishing Domain Detection & Takedown
- VIP Protection
- IoC Enrichment & SOAR Integration

Resources

- All-in-One Solution
- Blog
- Case Studies
- Newsletters
- Financial Data Breaches

Company

- About Us
- Partners
- Events
- Privacy Policy
- Information Security Policy
- Terms & Conditions and Refund Policy
- Free Services Terms & Conditions
- Contact Us

REQUEST DEMO
FREE ACCESS
FREE TOOLS