APT 29, Cozy Bear, The Dukes

Archived: 2026-04-05 18:36:11 UTC

APT group: APT 29, Cozy Bear, The Dukes

Names	APT 29 *(Mandiant)* Cozy Bear *(CrowdStrike)* The Dukes *(F-Secure)* Group 100 *(Talos)* Yttrium *(Microsoft)* Iron Hemlock *(SecureWorks)* Minidionis *(Palo Alto)* CloudLook *(Kaspersky)* ATK 7 *(Thales)* ITG11 *(IBM)* Grizzly Steppe *(US Government)* together with Sofacy, APT 28, Fancy Bear, Sednit UNC2452 *(FireEye)* Dark Halo *(Volexity)* SolarStorm *(Palo Alto)* StellarParticle *(CrowdStrike)* SilverFish *(Prodaft)* Nobelium *(Microsoft)* Iron Ritual *(SecureWorks)* Cloaked Ursa *(Palo Alto)* BlueBravo *(Recorded Future)* Midnight Blizzard *(Microsoft)* UNC3524 *(Mandiant)* Cranefly *(Symantec)* TEMP.Monkeys *(FireEye)* Blue Dev 5 *(PWC)* NobleBaron *(SentinelOne)* Solar Phoenix *(Palo Alto)* Earth Koshchei *(Trend Micro)* G0016 *(MITRE)*
Country	Russia
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2008
Description	(F-Secure) The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, pc and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of I Asian, African, and Middle Eastern governments; organizations associated with Chechen extremism; and Russian speakers illicit trade of controlled substances and drugs. The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionD CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently spear-phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and a organizations. These campaigns utilize a smash-and-grab approach involving a fast but noisy break-in followed by the rapid collection anc much data as possible. If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset use stealthier tactics focused on persistent compromise and long-term intelligence gathering.

	In addition to these large-scale campaigns, the Dukes continuously and concurrently engage in smaller, much more targeted utilizing different toolsets. These targeted campaigns have been going on for at least 7 years. The targets and timing of these to align with the known foreign and security policy interests of the Russian Federation at those times.	
Observed	Sectors: Aerospace, Defense, Education, Embassies, Energy, Financial, Government, Healthcare, Law enforcement, Media, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Imagery. Countries: Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chechnya, Chile, China, Cyprus, Czech, Den Georgia, Germany, Hungary, India, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxer Montenegro, Netherlands, New Zealand, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Slovenia, Spain, South K Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO.	
Tools used	7-Zip, AdFind, ATI-Agent, AtNow, BEATDROP, BloodHound, CEELOADER, CloudDuke, Cobalt Strike, CosmicDuke, C EnvyScout, FatDuke, FoggyWeb, GeminiDuke, Geppei, GoldFinder, GoldMax, GraphicalNeutrino, GraphicalProton, Hamı MagicWeb, meek, Mimikatz, MiniDuke, OnionDuke, PinchDuke, PolyglotDuke, POSHSPY, PowerDuke, QUIETEXIT, R/ RegDuke, reGeorg, Rubeus, SeaDuke, Sharp-SMBExec, SharpView, Sibot, SoreFang, SUNBURST, SUNSPOT, SUPERN(TrailBlazer, WellMail, WellMess, WINELOADER, Living off the Land.	
Operations performed	Feb 2013	Since the original announcement, we have observed several new attacks using the same exploit (CVE-2013-(other malware. Between these, we've observed a couple of incidents which are so unusual in many ways that analyse them in depth. <https://securelist.com/the-miniduke-mystery-pdf-0-day-government-spy-assembler-0x29a-micro-backdoor/
	2013	While the old style Miniduke implants were used to target mostly government victims, the new style Cosmic a somehow different typology of victims. The most unusual is the targeting of individuals that appear to be ir and reselling of controlled and illegal substances, such as steroids and hormones. These victims in the NITR(observed only in Russia. <https://securelist.com/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/64107/>
	2013	Operation "Ghost" We call these newly uncovered Dukes campaigns, collectively, Operation Ghost, and describe how the group compromising government targets, including three European Ministries of Foreign Affairs and the Washingtc European Union country, all without drawing attention to their activities. <https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf>
	Mar 2014	Operation "Office monkeys" In March 2014, a Washington, D.C.-based private research institute was found to have CozyDuke (Trojan.Cc network. Cozy Bear then started an email campaign attempting to lure victims into clicking on a flash video that would also include malicious executables. By July the group had compromised government networks an CozyDuke-infected systems to install MiniDuke onto a compromised network. <https://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory>
	Aug 2015	Attack on the Pentagon in the USA In August 2015 Cozy Bear was linked to a spear-phishing cyberattack against the Pentagon email system cau of the entire Joint Staff unclassified email system and Internet access during the investigation. <https://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html>
	Jun 2016	Breach of Democratic National Committee In June 2016, Cozy Bear was implicated alongside the hacker group Sofacy, APT 28, Fancy Bear, Sednit had few weeks. Cozy Bear's more sophisticated tradecraft and interest in traditional long-term espionage suggest originates from a separate Russian intelligence agency. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
	Aug 2016	Attacks on US think tanks and NGOs After the United States presidential election, 2016, Cozy Bear was linked to a series of coordinated and well- phishing campaigns against U.S.-based think tanks and non-governmental organizations (NGOs). <https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-tl ngos/>
	Jan 2017	Attacks on the Norwegian Government On February 3, 2017, the Norwegian Police Security Service (PST) reported that attempts had been made to email accounts of nine individuals in the Ministry of Defense, Ministry of Foreign Affairs, and the Labour Pa attributed to Cozy Bear, whose targets included the Norwegian Radiation Protection Authority, PST section c Haugstøyl, and an unnamed college. <https://www.usatoday.com/story/news/2017/02/03/norway-russian-hackers-hit-spy-agency-defense-labour-p

Feb 2017	Attack on Dutch ministries In February 2017, the General Intelligence and Security Service (AIVD) of the Netherlands revealed that Far Bear had made several attempts to hack into Dutch ministries, including the Ministry of General Affairs, ove months. Rob Bertholee, head of the AIVD, said on EenVandaag that the hackers were Russian and had tried t secret government documents. <https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-min>
Sep 2017	Russian hackers breached Dutch police systems in 2017 <https://therecord.media/russian-hackers-breached-dutch-police-systems-in-2017/>
Nov 2018	Phishing campaign in the USA Target: Multiple industries, including think tank, law enforcement, media, U.S. military, imagery, transportat national government, and defense contracting. Method: Phishing email appearing to be from the U.S. Department of State with links to zip files containing shortcuts that delivered Cobalt Strike Beacon. <https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-sus phishing-campaign.html>
Aug 2019	SolarWinds Orion Supply-chain Attack <https://www.dropbox.com/s/yu5uwsfyo9q4oj2/Whitepaper%20SolarWinds%20Orion%20Supply-chain%2(
Dec 2019	UNC3524: Eye Spy on Your Email <https://www.mandiant.com/resources/blog/unc3524-eye-spy-email>
2020	Throughout 2020, APT29 has targeted various organisations involved in COVID-19 vaccine development in States and the United Kingdom, highly likely with the intention of stealing information and intellectual prop development and testing of COVID-19 vaccines. <https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf>
2020	Suspected Russian Activity Targeting Government and Business Entities Around the Globe <https://www.mandiant.com/resources/russian-targeting-gov-business>
2021	Operation “StellarParticle” Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign <https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/>
Feb 2021	Russian cyberspies targeted the Slovak government for months <https://therecord.media/russian-cyberspies-targeted-slovak-government-for-months/>
Feb 2021	France warns of Nobelium cyberspies attacking French orgs <https://www.bleepingcomputer.com/news/security/france-warns-of-nobelium-cyberspies-attacking-french-c
Early 2021	Trello From the Other Side: Tracking APT29 Phishing Campaigns <https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns>
Apr 2021	FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor <https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persis
May 2021	Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns <https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phis
Jun 2021	New Nobelium activity <https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/>
Mid 2021	SOLARDEFLECTION C2 Infrastructure Used by NOBELIUM in Company Brand Misuse <https://www.recordedfuture.com/solardeflection-c2-infrastructure-used-by-nobelium-in-company-brand-mi
Jun 2021	Bear Tracks: Infrastructure Patterns Lead to More Than 30 Active APT29 C2 Servers <https://www.riskiq.com/blog/external-threat-management/apt29-bear-tracks/>
Jul 2021	Russia ‘Cozy Bear’ Breached GOP as Ransomware Attack Hit <https://www.bloomberg.com/news/articles/2021-07-06/russian-state-hackers-breached-republican-national-
Jul 2021	New activity from Russian actor Nobelium <https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/>
Jul 2021	Solarwind Attackers at It Again in Back-to-Back Campaigns <https://cybersecurityworks.com/blog/vulnerabilities/solarwind-attackers-at-it-again-in-back-to-back-campai

Jul 2021	In recent months, the Dukes launched several spearphishing campaigns targeting European diplomats, think t international organizations. ESET researchers identified victims in more than 12 different European countrie <https://www.welivesecurity.com/wp-content/uploads/2021/09/eset_threat_report_t22021.pdf>
Oct 2021	In October and November 2021, ESET detected additional spearphishing campaigns, again targeting Europe missions and Ministries of Foreign Affairs. <https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf>
Feb 2022	Nobelium Returns to the Political World Stage <https://www.fortinet.com/blog/threat-research/nobelium-returns-to-the-political-world-stage>
May 2022	Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive <https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/>
Aug 2022	You Can't Audit Me: APT29 Continues Targeting Microsoft 365 <https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft>
Aug 2022	MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone <https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-auth
Jan 2023	BlueBravo Adapts to Target Diplomatic Entities with GraphicalProton Malware <https://go.recordedfuture.com/hubfs/reports/cta-2023-0727-1.pdf>
Feb 2023	Diplomats Beware: Cloaked Ursa Phishing With a Twist <https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/>
Oct 2022	BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware <https://go.recordedfuture.com/hubfs/reports/cta-2023-0127.pdf>
Mar 2023	NOBELIUM Uses Poland's Ambassador's Visit to the U.S. to Target EU Governments Assisting Ukraine <https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine>
May 2023	Midnight Blizzard conducts targeted social engineering over Microsoft Teams <https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-eng microsoft-teams/>
May 2023	HPE: Russian hackers breached its security team's email accounts <https://www.bleepingcomputer.com/news/security/hpe-russian-hackers-breached-its-security-teams-email-a
Jun 2023	Kremlin-backed hacking group puts fresh emphasis on stealing credentials <https://therecord.media/nobelium-hacking-group-stealing-credentials>
Aug 2023	German Embassy Lure: Likely Part of Campaign Against NATO Aligned Ministries of Foreign Affairs <https://blog.eclecticiq.com/german-embassy-lure-likely-part-of-campaign-against-nato-aligned-ministries-o
Sep 2023	APT29 Attacks Embassies Using CVE-2023-38831 <https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/november/APT29%20attacks%20Embassies 2023-38831%20-%20report%20en.pdf>
Sep 2023	Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a>
Nov 2023	State-backed attackers and commercial surveillance vendors repeatedly use the same exploits <https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repe same-exploits/>
Jan 2024	Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnigh <https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-act blizzard/> <https://therecord.media/russia-hack-uk-government-home-office-microsoft>
Feb 2024	APT29 Uses WINELOADER to Target German Political Parties <https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties>
Jun 2024	TeamViewer's corporate network was breached in alleged APT hack <https://www.bleepingcomputer.com/news/security/teamviewers-corporate-network-was-breached-in-allege

	Oct 2024	Amazon identified internet domains abused by APT29 <https://aws.amazon.com/blogs/security/amazon-identified-internet-domains-abused-by-apt29/>
	Oct 2024	Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files <https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-p using-rdp-files/>
	Oct 2024	Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks <https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html>
	Jan 2025	Unmasking APT29: The Sophisticated Phishing Campaign Targeting European Diplomacy <https://blog.checkpoint.com/research/unmasking-apt29-the-sophisticated-phishing-campaign-targeting-eurc
	Feb 2025	Azerbaijan blames Russian state hackers for cyberattacks on local media <https://therecord.media/azerbaijan-blames-media-cyberattacks-russia-apt29>
Counter operations	Aug 2014	Dutch agencies provide crucial intel about Russia's interference in US-elections <https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-u elections~b4f8111b/>
	Jul 2018	Mueller indicts 12 Russians for DNC hacking as Trump-Putin summit looms <https://www.politico.com/story/2018/07/13/mueller-indicts-12-russians-for-hacking-into-dnc-718805>
	Apr 2021	Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the Governm Federation <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-h activities-by-the-russian-government/> <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/15/executive-order-on-blocking-p respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/> <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/a-letter-on-blocking-property-w specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/>
	Jun 2021	Justice Department Announces Court-Authorized Seizure of Domain Names Used in Furtherance of Spear-P Posing as U.S. Agency for International Development <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-seizure-domain-names-usec
Information	<https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf> <https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/> <https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/> <https://www.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf> <https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activ <https://exchange.xforce.ibmcloud.com/threat-group/guid:6acdb86af596b31ca8d273eb5572904f> <https://en.wikipedia.org/wiki/Cozy_Bear> <https://us-cert.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf> <https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf> <https://www.mandiant.com/resources/unc2452-merged-into-apt29> <https://www.mandiant.com/resources/blog/apt29-windows-credential-roaming> <https://raw.githubusercontent.com/prodaft/malware-ioc/master/SilverFish/SilverFish_TLPWHITE.pdf> <https://download.microsoft.com/download/4/6/5/4650b04f-7db6-4a87-bf82-8ed1ad1c001c/MS%20Security%20Experts%20Cyberattack%20MagicWeb%202023.pdf> <https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-att <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a> <https://therecord.media/france-anssi-warning-russia-hacking-campaign-svr> <https://www.ic3.gov/CSA/2024/241010.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0016/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=cloaked-ursa> <https://pan-unit42.github.io/playbook_viewer/?pb=solarphoenix>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format