Sofacy, APT 28, Fancy Bear, Sednit

APT group: Sofacy, APT 28, Fancy Bear, Sednit

Names	Sofacy *(Kaspersky)* APT 28 *(Mandiant)* Fancy Bear *(CrowdStrike)* Sednit *(ESET)* Group 74 *(Talos)* TG-4127 *(SecureWorks)* Pawn Storm *(Trend Micro)* Tsar Team *(iSight)* Strontium *(Microsoft)* Swallowtail *(Symantec)* SIG40 *(NSA)* Snakemackerel *(iDefense)* Iron Twilight *(SecureWorks)* ATK 5 *(Thales)* T-APT-12 *(Tencent)* ITG05 *(IBM)* TAG-0700 *(Recorded Future)* UAC-0028 *(CERT-UA)* FROZENLAKE *(Google)* Grey-Cloud *(?)* Grizzly Steppe *(US Government)* together with APT 29, Cozy Bear, The Dukes Forest Blizzard *(Microsoft)* GruesomeLarch *(Volexity)* BlueDelta *(Recorded Future)* TA422 *(Proofpoint)* Fighting Ursa *(Palo Alto)* Blue Athena *(PWC)* UAC-0063 *(CERT-UA)* TAG-110 *(Recorded Future)* G0007 *(MITRE)*
Country	Russia
Sponsor	State-sponsored, two GRU units known as Unit 26165 and Unit 74455
Motivation	Information theft and espionage
First seen	2004
Description	APT 28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian Gen Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary C campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2 an attempt to interfere with the U.S. presidential election. APT 28 has been active since at least January 2007.

	(FireEye) APT28 likely seeks to collect intelligence about Georgia's security and political dynamics by targeti officials working for the Ministry of Internal Affairs and the Ministry of Defense. APT28 has demonstrated interest in Eastern European governments and security organizations. These victims provide the Russian government with an ability to predict policymaker intentions and gauge its ability to influ public opinion. APT28 appeared to target individuals affiliated with European security organizations and global multilateral institutions. The Russian government has long cited European security organizations like NATO and the OSC existential threats, particularly during periods of increased tension in Europe. Sofacy may be related to Hades, but it could be a false flag as well.	
Observed	Sectors: Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Energy, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations. Countries: Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, C Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Italy, Japan, Jordan, Kazakhstan, Latvi Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Saudi Arabia, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE Ukraine, USA, Uzbekistan, NATO and APEC and OSCE.	
Tools used	Cannon, certutil, CHERRYSPY, Computrace, CORESHELL, DealersChoice, Downdelph, Drovorub, Foozer, GooseEgg, Graphite, HATVIBE, Headlace, HIDEDRV, Impacket, JHUHUGIT, Koadic, Komplex, LoJax, MASEPIE, Mimikatz, Nimcy, OCEANMAP, OLDBAIT, PocoDown, ProcDump, PythocyDbg, Responder, Se Sedreco, SkinnyBoy, SMBExec, STEELHOOK, USBStealer, VPNFilter, Winexe, WinIDS, X-Agent, X-Tunn Zebrocy, Living off the Land.	
Operations performed	2011/2012	Back in 2011-2012, the group used a relatively tiny implant (known as "Sofacy" or SOURFAC its first stage malware. The implant shared certain similarities with the old Miniduke implants. led us to believe the two groups were connected, at least to begin with, although it appears they parted ways in 2014, with the original Miniduke group switching to the CosmicDuke implant.
	2013	At some point during 2013, the Sofacy group expanded its arsenal and added more backdoors a tools, including CORESHELL, SPLM (aka Xagent, aka CHOPSTICK), JHUHUGIT (which is with code from the Carberp sources), AZZY (aka ADVSTORESHELL, NETUI, EVILTOSS, a spans across four to five generations) and a few others. We've seen quite a few versions of thes implants and they were relatively widespread for a time.
	Oct 2014	Operation "Pawn Storm" Target: Several foreign affairs ministries from around the globe. Method: Spear-phishing e-mails with links leading to an Adobe Flash exploit. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-i pawn-storm-campaign/>
	Dec 2014	Six-month-long cyberattack on the German parliament <http://www.lse.co.uk/AllNews.asp?code=kwdwehme&headline=Russian_Hackers_Suspected_In_Cyberattack_On_German_Parli
	Feb 2015	U.S. military wives' death threats Five military wives received death threats from a hacker group calling itself "Cyber Caliphate (CCA), United Cyber Caliphate (UCC)", claiming to be an Islamic State affiliate, on February 2015. This was later discovered to have been a false flag attack by Fancy Bear, when the victim email addresses were found to have been in the Fancy Bear phishing target list. <https://www.apnews.com/4d174e45ef5843a0ba82e804f080988f>

Apr 2015	Compromise of TV5Monde in France “A group calling itself the Cyber Caliphate Army (CCA), United Cyber Caliphate (UCC), linke so-called Islamic State, first claimed responsibility. But an investigation now suggests the attac in fact carried out by a group of Russian hackers.” <https://www.bbc.com/news/technology-37590375>
Apr 2015	Operation “Russian Doll” Method: Adobe Flash 0-day <https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html>
Apr 2015	Compromise of the German Parliament (Bundestag) network <https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-h of-the-left-party-infrastructure-in-bundestag/>
Jul 2015	Pawn Storm Update: Trend Micro Discovers New Java Zero-Day Exploit <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-trend-micro-discovers-new-java-zero-day-exploit/>
Aug 2015	EFF spoof, White House and NATO attack Method: zero-day exploit of Java, spoofing the Electronic Frontier Foundation and launching a on the White House and NATO. The hackers used a spear-phishing attack, directing emails to th false url electronicfrontierfoundation.org. <https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff>
Sep 2015	Bootstrapped Firefox Add-on <https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/>
Oct 2015	Attack on Bellingcat Eliot Higgins and other journalists associated with Bellingcat, a group researching the shoot do Malaysia Airlines Flight 17 over Ukraine, were targeted by numerous spear-phishing emails. Th messages were fake Gmail security notices with Bit.ly and TinyCC shortened URLs. <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investig team/>
Oct 2015	Attack on Dutch Safety Board The group targeted the Dutch Safety Board, the body conducting the official investigation into crash, before and after the release of the board’s final report. They set up fake SFTP and VPN s to mimic the board’s own servers, likely for the purpose of spear-phishing usernames and passv <https://www.msn.com/en-au/news/world/russia-tried-to-hack-mh17-inquiry-system/ar-BBmm
Oct 2015	New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministri <https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in pawn-storm-campaign/>
Jan 2016	Pawn Storm Campaign Adds Turkey To Its List of Targets <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-adds-turkey-list-targe
May 2016	Pawn Storm Targets German Christian Democratic Union <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christ democratic-union/>
May 2016	Russian cyber-espionage group hits Sanoma <https://yle.fi/uutiset/osasto/news/russian_cyber-espionage_group_hits_sanoma/8919118>
Jun 2016	Breach of Democratic National Committee Fancy Bear carried out spear-phishing attacks on email addresses associated with the Democrat National Committee in the first quarter of 2016. On March 10, phishing emails that were mainl

	directed at old email addresses of 2008 Democratic campaign staffers began to arrive. One of tl accounts may have yielded up to date contact lists. The next day, phishing attacks expanded to non-public email addresses of high level Democratic Party officials. Hillaryclinton.com addres were attacked, but required two factor authentication for access. The attack redirected towards accounts on March 19th. Podesta's Gmail account was breached the same day, with 50,000 em stolen. Another sophisticated hacking group attributed to the Russian Federation, nicknamed APT 29, Bear, The Dukes appears to be a different agency, one more interested in traditional long-term espionage. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> <https://www.secureworks.com/research/threat-group-4127-targets-google-accounts>
Jun 2016	"Exercise Noble Partner 2016" spear-phishing e-mail Method: Spear-phishing e-mail Target: USA government <https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agenc
Aug 2016	Spear-phishing attack members of the Bundestag and multiple political parties such as Linken- leader Sahra Wagenknecht, Junge Union and the CDU of Saarland. Authorities feared that sens information could be gathered by hackers to later manipulate the public ahead of elections such Germany's next federal election which was due in September 2017. <http://www.dw.com/en/hackers-lurking-parliamentarians-told/a-19564630>
Aug 2016	World Anti-Doping Agency Method: Phishing emails sent to users of its database claiming to be official WADA communic requesting their login details. <http://www.ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-a dnc-experts-say-1577508>
Sep 2016	Operation "Komplex" <https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/>
Oct 2016	Operation "DealersChoice" <https://unit42.paloaltonetworks.com/unit42-dealerschoice-sofacys-flash-player-exploit-platfo <https://unit42.paloaltonetworks.com/unit42-let-ride-sofacy-groups-dealerschoice-attacks-cont The global reach that coincided with this focus on NATO and the Ukraine couldn't be overstate KSN data showed spear-phishing targets geo-located across the globe into 2017. AM, AZ, FR, DE, IQ, IT, KG, MA, CH, UA, US, VN DealersChoice emails, like the one above, that we were able to recover from third party sources provided additional targeting insight, and confirmed some of the targeting within our KSN data TR, PL, BA, AZ, KR, LV, GE, LV, AU, SE, BE
Early 2017	GAMEFISH backdoor Target: Europe. Method: They took advantage of the Syrian military conflict for thematic content and file nami "Trump's_Attack_on_Syria_English.docx". Again, this deployment was likely a part of their fo NATO targets.
Early 2017	LoJax: First UEFI rootkit found in the wild <https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sedn group/>
Feb 2017	Attack on Dutch ministries In February 2017, the General Intelligence and Security Service (AIVD) of the Netherlands rev that Fancy Bear and Cozy Bear had made several attempts to hack into Dutch ministries, includ

	the Ministry of General Affairs, over the previous six months. Rob Bertholee, head of the AIVI on EenVandaag that the hackers were Russian and had tried to gain access to secret governmen documents. <https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries~b77ff391/>
Feb 2017	Russian Hackers 'Fancy Bear' Targeted French Presidential Candidate Macron <https://www.vice.com/en_us/article/ez35p7/russian-hackers-fancy-bear-targeted-french-presid candidate-macron>
Feb 2017	IAAF Hack The officials of International Association of Athletics Federations (IAAF) stated in April 2017 t servers had been hacked by the "Fancy Bear" group. The attack was detected by cybersecurity Context Information Security which identified that an unauthorized remote access to IAAF's se had taken place on February 21. IAAF stated that the hackers had accessed the Therapeutic Use Exemption applications, needed to use medications prohibited by WADA. <https://www.voanews.com/a/iaaf-hack-fancy-bears/3793874.html>
Apr 2017	German elections They targeted the German Konrad Adenauer Foundation and Friedrich Ebert Foundation, group are associated with Angela Merkel's Christian Democratic Union and opposition Social Democ Party, respectively. Fancy Bear set up fake email servers in late 2016 to send phishing emails w links to malware. <https://www.handelsblatt.com/today/politics/election-risks-russia-linked-hackers-target-germa political-foundations/23569188.html?ticket=ST-2696734-GRHgtQukDIEXeSOwksXO-ap1>
Early 2017	SPLM backdoor Target: included defense related commercial and military organizations, and telecommunicatior Targeting included TR, KZ, AM, KG, JO, UK, UZ Method: SPLM/CHOPSTICK/Xagent
Jun 2017	Heavy Zebrocy deployments Targeting profiles, spear-phish filenames, and lures carry thematic content related to visa applic and scanned images, border control administration, and various administrative notes. Targeting appears to be widely spread across the Middle East, Europe, and Asia: - Business accounting practices and standards - Science and engineering centers - Industrial and hydro chemical engineering and standards/certification - Ministry of foreign affairs - Embassies and consulates - National security and intelligence agencies - Press services - Translation services - NGO – family and social service - Ministry of energy and industry Method: the Zebrocy chain follows a pattern: spear-phish attachment -> compiled Autoit script (downloader) -> Zebrocy payload. In some deployments, we observed Sofacy actively develop and deploying a new package to a much smaller, specific subset of targets within the broader se
Jul 2017	APT28 Targets Hospitality Sector, Presents Threat to Travelers <https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html>
Oct 2017	In this case it capitalized on the recent terrorist attack in New York City. The document itself is Once opened, the document contacts a control server to drop the first stage of the malware, Seduploader, onto a victim's system.

	<https://securingtomorrow.mcafee.com/mcafee-labs/apt28-threat-group-adopts-dde-technique-attack-theme-in-latest-campaign/#sf151634298>
Oct 2017	Russische hackers vallen vredesbeweging Pax aan <https://www.human.nl/schimmenspel/russische-hackers-vallen-Nederlandse-vredesbeweging-aan.html>
Jan 2018	Breach of the International Olympic Committee On January 10, 2018, the “Fancy Bears Hack Team” online persona leaked what appeared to be stolen International Olympic Committee (IOC) and U.S. Olympic Committee emails, dated from 2016 to early 2017, were leaked in apparent retaliation for the IOC’s banning of Russian athletes from the 2018 Winter Olympics as a sanction for Russia’s systematic doping program. The attack resembles the earlier World Anti-Doping Agency (WADA) leaks. It is not known whether the emails are fully authentic, because of Fancy Bear’s history of salting stolen emails with disinformation. The mode of attack was also not known, but was probably phishing. <https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/>
Feb 2018	Attacks on Multiple Government Entities Target: Ministries of Foreign Affairs of the USA and Romania. Method: Spear-phishing using the subject line of Upcoming Defense events February 2018 and sender address claiming to be from Jane’s 360 defense events. <https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/>
Mar 2018	On March 12 and March 14, we observed the Sofacy group carrying out an attack on a European government agency involving an updated variant of DealersChoice. The updated DealersChoice documents used a similar process to obtain a malicious Flash object from a C2 server, but the internal mechanics of the Flash object contained significant differences in comparison to the original sample we analyzed. <https://unit42.paloaltonetworks.com/unit42-sofacy-uses-dealerschoice-target-european-government-agency/>
May 2018	Breach of the Swedish Sports Confederation The Swedish Sports Confederation reported Fancy Bear was responsible for an attack on its computers, targeting records of athletes’ doping tests. <https://www.reuters.com/article/us-sweden-doping/swedish-sports-body-says-anti-doping-unit-by-hacking-attack-idUSKCN1IG2GN>
May 2018	VPNFilter IoT botnet ThaiCERT's whitepaper: <https://www.dropbox.com/s/9lkeenhveb3xbkq/Whitepaper VPNFilter IoT botnet seized by the FBI.pdf?dl=0>
Jun 2018	This third campaign is consistent with two previously reported attack campaigns in terms of targeting: the targets were government organizations dealing with foreign affairs. In this case however the targets were in different geopolitical regions. <https://unit42.paloaltonetworks.com/unit42-sofacy-groups-parallel-attacks/>
Aug 2018	Attacks on United States Conservative Groups The software company Microsoft reported in August 2018 that the group had attempted to steal from political organizations such as the International Republican Institute and the Hudson Institute think tanks. The attacks were thwarted when Microsoft security staff won control of six net domains. In its announcement Microsoft advised that “we currently have no evidence these domains were in any successful attacks before the DCU transferred control of them, nor do we have evidence to indicate the identity of the ultimate targets of any planned attack involving these domains”. <https://www.bbc.co.uk/news/technology-45257081>

Oct 2018	Operation “Dear Joohn” Target: The weaponized documents targeted several government entities around the globe, inclu North America, Europe, and a former USSR state. Method: new ‘Cannon’ Trojan <https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/> <https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-canr trojan/>
2018	BREXIT-themed lure document Brexit-themed bait documents to deliver the Zekapab (also known as Zebrocy) first-stage malw sent on the same day the UK Prime Minister Theresa May announced the initial BREXIT draft agreement with the European Union (EU). “As the United Kingdom (UK) Prime Minister Ther May announced the initial BREXIT draft agreement with the European Union (EU). <https://www.accenture.com/t20181129T203820Z__w__/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf>
Feb 2019	2019 Think Tank Attacks In February 2019, Microsoft announced that it had detected spear-phishing attacks from APT28 aimed at employees of the German Marshall Fund, Aspen Institute Germany, and the German Council on Foreign Relations. Hackers from the group purportedly sent phishing e-mails to 10 addresses across Europe in an attempt to gain access to employer credentials and infect sites wi malware. <https://www.washingtonpost.com/technology/2019/02/20/microsoft-says-it-has-found-anothe russian-operation-targeting-prominent-think-tanks/?utm_term=.870ff11468ae>
Feb 2019	Threat Campaign Likely Targeting NATO Members, Defense and Military Outlets iDefense assesses with moderate confidence that the actors may be targeting attendees and spor of the upcoming Underwater Defense & Security 2019 event occurring March 5-7, 2019, in Southampton, United Kingdom. This event draws attendees from government, military and priv sector entities across the globe. <https://www.accenture.com/t20190213T141124Z__w__/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Milit Outlets.pdf>
Apr 2019	In April, security researchers in the Microsoft Threat Intelligence Center discovered infrastructu a known adversary communicating to several external devices. Further research uncovered atte by the actor to compromise popular IoT devices (a VOIP phone, an office printer, and a video decoder) across multiple customer locations. <https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/>
Apr 2019	Analyzing Forest Blizzard’s custom post-compromise tool for exploiting CVE-2022-38028 to c credentials <https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/>
May 2019	Since May 2019, Pawn Storm has been abusing compromised email addresses to send credentia phishing spam. The majority of the compromised systems were from defense companies in the Middle East. Other targets included organizations in the transportation, utilities, and governmer sectors. <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/probing-pawn-storm-cyberespionage-campaign-through-scanning-credential-phishing-and-more>

Aug 2019	On August 20th, 2019, a new campaign was launched by the group targeting their usual victims embassies of, and Ministries of Foreign Affairs in, Eastern European and Central Asian countri <https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/>
Aug 2019	APT28, one of Russia's military hacking units, was most likely responsible for hacking the ema accounts of the Norwegian Parliament, the Norwegian police secret service (PST) said today. <https://www.zdnet.com/article/norway-says-russian-hacking-group-apt28-is-behind-august-20 parliament-hack/>
Sep 2019	At least 16 national and international sporting and anti-doping organizations across three contir were targeted in these attacks which began September 16th, just before news reports about new potential action being taken by the World Anti-Doping Agency. Some of these attacks were successful, but the majority were not. <https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/>
Nov 2019	Beginning in early November of 2019, the Main Intelligence Directorate of the General Staff o Russian Army (GRU) launched a phishing campaign targeting Burisma Holdings, a holding cor of energy exploration and production companies based in Kiev, Ukraine. <https://cdn.area1security.com/reports/Area-1-Security-PhishingBarismaHoldings.pdf>
Apr 2020	Microsoft has tied STRONTIUM to a newly uncovered pattern of Office365 credential harvesti activity aimed at US and UK organizations directly involved in political elections. <https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-creden harvesting/>
May 2020	Pawn Storm scanned IP addresses worldwide, including IP addresses from the defense industry Europe, on TCP port 445 and 1433, likely in an attempt to find vulnerable SMB and SQL serve brute force credentials. <https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html>
Aug 2020	New cyberattacks targeting U.S. elections <https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/
Aug 2020	APT28 Delivers Zebrocy Malware Campaign using NATO Theme as Lure <https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/>
Nov 2020	A Zebra in Gopher's Clothing: Russian APT Uses COVID-19 Lures to Deliver Zebrocy <https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/>
2021	France says Russian state hackers breached numerous critical networks <https://www.bleepingcomputer.com/news/security/france-says-russian-state-hackers-breached numerous-critical-networks/>
Jun 2021	A not so Fancy game. Exploring the new “SkinnyBoy” Bear’s backdoor <https://cluster25.io/wp-content/uploads/2021/05/2021-05_FancyBear.pdf>
Jun 2021	Hackers Exploited MSHTML Flaw to Spy on Government and Defense Targets <https://thehackernews.com/2022/01/hackers-exploited-mshtml-flaw-to-spy-on.html>
Sep 2021	Google notifies 14,000 Gmail users of targeted APT28 attacks <https://therecord.media/google-notifies-14000-gmail-users-of-targeted-apt28-attacks/>
Feb 2022	The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for C Access <https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/>

Feb 2022	FancyBear/APT28, a threat actor attributed to Russia GRU, has conducted several large creden phishing campaigns targeting ukr.net users, UkrNet is a Ukrainian media company. <https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/>
Feb 2022	BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Acti <https://go.recordedfuture.com/hubfs/reports/cta-2023-0620.pdf>
Apr 2022	APT28 or Fancy Bear, a threat actor attributed to Russia GRU, was observed targeting users in Ukraine with a new variant of malware. <https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/>
Apr 2022	Pawn Storm Uses Brute Force and Stealth Against High-Value Targets <https://www.trendmicro.com/en_us/research/24/a/pawn-storm-uses-brute-force-and-stealth.ht
Jun 2022	The Ukrainian Computer Emergency Response Team (CERT) is warning that Russian hacking are exploiting the Follina code execution vulnerability in new phishing campaigns to install the CredoMap malware and Cobalt Strike beacons. <https://www.bleepingcomputer.com/news/security/russian-govt-hackers-hit-ukraine-with-cob strike-credomap-malware/>
Sep 2022	In the footsteps of the Fancy Bear: PowerPoint mouse-over event abused to deliver Graphite im <https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint graphite/>
Mar 2023	TA422's Dedicated Exploitation Loop—the Same Week After Week <https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-v after-week>
Apr 2023	Hackers use fake 'Windows Update' guides to target Ukrainian govt <https://www.bleepingcomputer.com/news/security/hackers-use-fake-windows-update-guides-t target-ukrainian-govt/>
Apr 2023	GRU's BlueDelta Targets Key Networks in Europe with Multi-Phase Espionage Campaigns <https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf>
Aug 2023	ITG05 operations leverage Israel-Hamas conflict lures to deliver Headlace malware <https://securityintelligence.com/x-force/itg05-ops-leverage-israel-hamas-conflict-lures-to-deli headlace-malware/>
Sep 2023	Ukraine says an energy facility disrupted a Fancy Bear intrusion <https://therecord.media/ukraine-energy-facility-cyberattack-fancy-bear-email>
Sep 2023	Fighting Ursa Aka APT28: Illuminating a Covert Campaign <https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/>
Sep 2023	Operation "Steal-It" <https://www.zscaler.com/blogs/security-research/steal-it-campaign>
Sep 2023	Operation "RoundPress" <https://www.welivesecurity.com/en/eset-research/operation-roundpress/>
Dec 2023	Russian hackers exploiting Outlook bug to hijack Exchange accounts <https://www.bleepingcomputer.com/news/microsoft/russian-hackers-exploiting-outlook-bug-t hijack-exchange-accounts/>
Dec 2023	Russian military hackers target Ukraine with new MASEPIE malware <https://www.bleepingcomputer.com/news/security/russian-military-hackers-target-ukraine-wit new-masepie-malware/>

	Feb 2024	Russian hackers hijack Ubiquiti routers to launch stealthy attacks <https://www.bleepingcomputer.com/news/security/russian-hackers-hijack-ubiquiti-routers-to-launch-stealthy-attacks/>
	Mar 2024	Ongoing ITG05 operations leverage evolving malware arsenal in global campaigns <https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/>
	Mar 2024	Fighting Ursa Luring Targets With Car for Sale <https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/>
	Mar 2024	APT28 hackers use Signal chats to launch new malware attacks on Ukraine <https://www.bleepingcomputer.com/news/security/apt28-hackers-use-signal-chats-to-launch-r malware-attacks-on-ukraine/>
	Early 2024	MITRE: Russian APT28's LameHug, a Pilot for Future AI Cyber-Attacks <https://www.infosecurity-magazine.com/news/mitre-russian-apt28-lamehug/>
	May 2024	Poland says Russian military hackers target its govt networks <https://www.bleepingcomputer.com/news/security/poland-says-russian-military-hackers-targe govt-networks/>
	Jul 2024	Ukrainian Institutions Targeted Using HATVIBE and CHERRYSPY Malware <https://thehackernews.com/2024/07/ukrainian-institutions-targeted-using.html>
	Jul 2024	Russia-Aligned TAG-110 Targets Asia and Europe with HATVIBE and CHERRYSPY <https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-1121.pdf>
	Sep 2024	German Cyber Agency Investigating APT28 Phishing Campaign <https://www.bankinfosecurity.com/german-cyber-agency-investigating-apt28-phishing-campa 26234>
	Sep 2024	French Cyber Agency Warns of APT28 Hacks Against Think Tanks <https://www.bankinfosecurity.com/french-cyber-agency-warns-apt28-hacks-against-think-tanl 26265>
	Sep 2024	UAC-0063: Cyber Espionage Operation Expanding from Central Asia <https://www.bitdefender.com/en-us/blog/businessinsights/uac-0063-cyber-espionage-operatio expanding-from-central-asia>
	Oct 2024	Double-Tap Campaign: Russia-nexus APT possibly related to APT28 conducts cyber espionage Central Asia and Kazakhstan diplomatic relations <https://blog.sekoia.io/double-tap-campaign-russia-nexus-apt-possibly-related-to-apt28-conduc cyber-espionage-on-central-asia-and-kazakhstan-diplomatic-relations/>
	Jan 2025	Russia-Aligned TAG-110 Targets Tajikistan with Macro-Enabled Word Templates <https://go.recordedfuture.com/hubfs/reports/cta-2025-0522.pdf>
Counter operations	May 2018	Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Inf Routers and Network Storage Devices <https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persis threat-28-botnet-infected>
	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>
	Aug 2018	Microsoft’s Digital Crimes Unit (DCU) successfully executed a court order to disrupt and trans control of six internet domains

		<https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broad threats-to-democracy/>
	Oct 2018	US charges Russian military officers over international hacking and disinformation campaigns <https://www.zdnet.com/article/us-charges-russian-military-officers-over-international-hacking disinformation-campaigns/>
	May 2020	German authorities charge Russian hacker for 2015 Bundestag hack <https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/>
	Apr 2022	Disrupting cyberattacks targeting Ukraine <https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/>
	Apr 2023	Hacked: Russian GRU officer wanted by the FBI, leader of the hacker group APT 28 <https://informnapalm.org/en/hacked-russian-gru-officer/>
	Jan 2024	Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) <https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botn controlled-russian>
	Apr 2025	France ties Russian APT28 hackers to 12 cyberattacks on French orgs <https://www.bleepingcomputer.com/news/security/france-ties-russian-apt28-hackers-to-12-cyberattacks-on-french-orgs/>
Information	<https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/> <http://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf> <https://securelist.com/a-slice-of-2017-sofacy-activity/83930/> <https://www.symantec.com/blogs/election-security/apt28-espionage-military-government> <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> <https://threatvector.cylance.com/en_us/home/flirting-with-ida-and-apt28.html> <https://threatvector.cylance.com/en_us/home/inside-the-apt28-dll-backdoor-blitz.html> <https://securelist.com/zebrocys-multilanguage-malware-salad/90680/> <https://marcoramilli.com/2019/12/05/apt28-attacks-evolution/> <https://www.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.p <https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf> <https://exchange.xforce.ibmcloud.com/threat-group/guid:f7b33aa456eb38053abd85968f78833a> <https://en.wikipedia.org/wiki/Fancy_Bear> <https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf> <https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/> <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/> <https://www.trendmicro.com/en_us/research/24/e/router-roulette.html> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a> <https://www.cyfirma.com/research/apt-profile-fancy-bear-2/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0007/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=fighting-ursa>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
