Sandworm Team, Iron Viking, Voodoo Bear

Archived: 2026-04-05 19:43:13 UTC

APT group: Sandworm Team, Iron Viking, Voodoo Bear

Names	Sandworm Team *(Trend Micro)* Sandworm *(ESET)* Iron Viking *(SecureWorks)* CTG-7263 *(SecureWorks)* Voodoo Bear *(CrowdStrike)* Quedagh *(F-Secure)* TEMP.Noble *(FireEye)* ATK 14 *(Thales)* BE2 *(Kaspersky)* UAC-0082 *(CERT-UA)* UAC-0113 *(CERT-UA)* UAC-0125 *(CERT-UA)* UAC-0133 *(CERT-UA)* FROZENBARENTS *(Google)* IRIDIUM *(Microsoft)* Seashell Blizzard *(Microsoft)* APT 44 *(Mandiant)* Blue Echidna *(PwC)* Grey Tornado *(?)* Razing Ursa *(Palo Alto)* G0034 *(MITRE)*
Country	Russia
Sponsor	State-sponsored, GRU Unit 74455
Motivation	Sabotage and destruction
First seen	2009
Description	Sandworm Team is a Russian cyberespionage group that has operated since approximately 2009. The group likely consists of Russian pro-hacktivists. Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media. Sandworm Team has been linked to the Ukrainian energy sector attack in late 2015.

	This group appears to be closely associated with, or evolved into, TeleBots.	
Observed	Sectors: Education, Energy, Government, Industrial, Telecommunications. Countries: Afghanistan, Angola, Argentina, Australia, Austria, Azerbaijan, Belarus, Belgium, Bulgaria, Cambodia, Canada, China, Colombia, Czech, Denmark, Egypt, France, Georgia, Germany, Ghana, Hungary, India, Iran, Israel, Italy, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Moldova, Myanmar, Netherlands, Nigeria, Oman, Norway, Pakistan, Paraguay, Peru, Poland, Portugal, Romania, Russia, Serbia, South Korea, Spain, Sweden, Syria, Thailand, Turkey, UK, Ukraine, USA, Uzbekistan, Vietnam.	
Tools used	ArguePatch, AWFULSHRED, BIASBOAT, BlackEnergy, CaddyWiper, Chisel, Colibri Loader, Cyclops Blink, DarkCrystal RAT, Gcat, GOSSIPFLOW, Industroyer2, JuicyPotato, LOADGRIP, ORCSHRED, P.A.S., PassKillDisk, Pitvotnacci, PsList, QUEUESEED, RansomBoggs, RottenPotato, SOLOSHRED, SwiftSlicer, VPNFilter, Warzone RAT, Weevly, Living off the Land.	
Operations performed	Oct 2014	The vulnerability was disclosed by iSIGHT Partners, which said that the vulnerability had already been exploited in a small number of cyberespionage attacks against NATO, several unnamed Ukrainian government organizations, a number of Western European governmental organizations, companies operating in the energy sector, European telecoms firms, and a US academic organization. <https://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks>
	Dec 2015	Widespread power outages on the Ukraine The power outage was described as technical failures taking place on Wednesday, December 23 that impacted a region around Ivano-Frankivisk Oblast. One report suggested the utility began to disconnect power substations for no apparent reason. The same report goes on to describe a virus was launched from the outside and it brought down the “remote management system” (a reference to the SCADA and or EMS). The outage was reported to have lasted six hours before electrical service was restored. At least two reports suggest the utility had initiated manual controls for restoration of service and the SCADA system was still off-line due to the infection. <https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage>
	Late 2017	ANSSI has been informed of an intrusion campaign targeting the monitoring software Centreon distributed by the French company

	CENTREON which resulted in the breach of several French entities. <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf>
Jun 2019	New Sandworm Malware Cyclops Blink Replaces VPNFilter <https://www.cisa.gov/uscert/ncas/alerts/aa22-054a>
Aug 2019	Russian military cyber actors, publicly known as Sandworm Team, have been exploiting a vulnerability in Exim mail transfer agent (MTA) software since at least last August. <https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/>
2021	The BadPilot campaign: Seashell Blizzard subgroup conducts multiyear global access operation <https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/>
Apr 2022	Industroyer2: Industroyer reloaded <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>
May 2022	Sandworm uses a new version of ArguePatch to attack targets in Ukraine <https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/>
Jun 2022	Russian hackers start targeting Ukraine with Follina exploits <https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/>
Jun 2022	Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology <https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology>
Aug 2022	Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine <https://go.recordedfuture.com/hubfs/reports/cta-2022-0919.pdf>
Nov 2022	RansomBoggs: New ransomware targeting Ukraine <https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/>

	Jan 2023	SwiftSlicer: New destructive wiper malware strikes Ukraine <https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/>
	Apr 2023	Russian hackers use WinRAR to wipe Ukraine state agency's data <https://www.bleepingcomputer.com/news/security/russian-hackers-use-winrar-to-wipe-ukraine-state-agencys-data/>
	Apr 2023	The attack against Danish critical infrastructure <https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf>
	May 2023	Russian Sandworm hackers breached 11 Ukrainian telcos since May <https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-breached-11-ukrainian-telcos-since-may/>
	May 2023	Russian hackers wiped thousands of systems in KyivStar attack <https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/> <https://therecord.media/kyivstar-ceo-on-russian-cyberattack-telecom>
	Late 2023	Sandworm APT Targets Ukrainian Users with Trojanized Microsoft KMS Activation Tools in Cyber Espionage Campaigns <https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns>
	Mar 2024	Russian Sandworm hackers targeted 20 critical orgs in Ukraine <https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-targeted-20-critical-orgs-in-ukraine/>
	Dec 2024	Sandworm-linked hackers target users of Ukraine's military app in new spying campaign <https://therecord.media/ukraine-military-app-espionage-russia-sandworm>
Counter operations	Oct 2020	Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>
	Apr 2022	Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)

		<https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/> <https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/> <https://www.welivesecurity.com/2022/03/21/sandworm-tale-disruption-told-anew/> <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://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0034/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
