Advanced Persistent Threat 44 (APT44): An Intelligence Assessment of Russia's "Sandworm" Cyber Sabotage Unit

Cyber Intelligence Report

by

Solomon Neas

October 19, 2025

Executive Summary

Advanced Persistent Threat 44 (APT44), also known as Sandworm, is a highly active and operationally mature Russian state-sponsored threat actor. It functions as a versatile tool for the Kremlin, conducting a full spectrum of espionage, attack, and influence operations to support Russia's national interests, aid military efforts, and undermine democratic processes globally. While Ukraine has been the primary focus of its most destructive and disruptive attacks over the past decade, APT44 maintains a global mandate, targeting government, defense, and energy sectors worldwide, including critical infrastructure in North America and Europe. The group's methodology is adaptable, ranging from deploying destructive wiper malware like NotPetya and abusing native system tools ("Living off the Land") to exploiting edge infrastructure. To amplify the psychological impact of its operations, APT44 also creates and manages hacktivist front personas, such as the Cyber Army of the Russia Reborn (CARR), to publicly claim responsibility for its attacks

Actor(s)

APT44 is a Russian Federation-backed threat group formally attributed by multiple governments to Unit 74455 of the Main Center for Special Technologies (GtsST) within the Main Intelligence Directorate (GRU). This advanced threat actor is sponsored by Russian military intelligence and is actively engaged in the full spectrum of cyber espionage, attack, and influence operations, serving as the main cyber attack unit within the GRU. APT44 operations reflect Russia's core concept of "information confrontation" in cyber warfare, and the group is viewed by the Kremlin as a flexible instrument of power serving broad national interests.

To amplify its influence operations and publicly claim disruptive acts for psychological impact, APT44 utilizes various front personas embedded within the pro-Russian Telegram ecosystem. These personas include CARR (which Mandian assesses with high confidence is orchestrated and managed by APT44 operators), XakNet Team, and Solntsepek. Furthermore, APT44 and its front personas frequently engage in collaborative efforts and alliance with other pro-Russian hacktivist groups, such as NoName057(16), HackNeT, and others like UserSec. NoName057(16) is a pro-Russian hacktivist group specializing in Distributed Denial-of-Service (DDoS) attacks against Ukraine, NATO members, and their allies. This strategy of coordination with groups like NoName057(16) expands APT44's

reach and enhances operational deniability, thereby maintaining APT44's standing as a persistent, high-severity threat to governments and critical infrastructure worldwide.

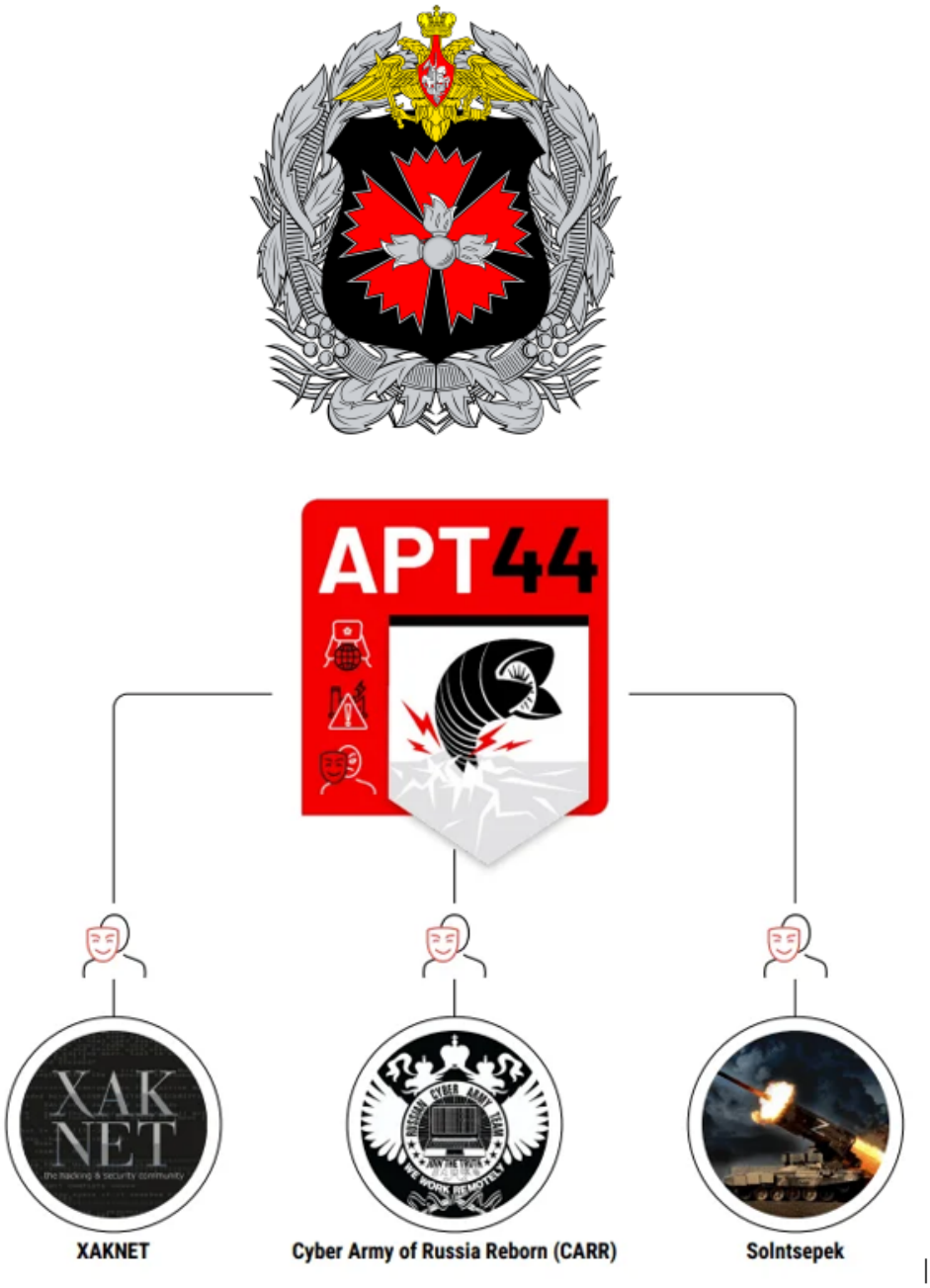

Image Source: Mandiant

Target(s)

APT44 maintains a broad, global targeting mandate, mainly focusing on government, defense, transportation, energy, media, and civil society organizations. While Ukraine remains the primary focus of APT44's operations due to Russia's geopolitical goals, the group's activities are worldwide, including North America, Europe, the Middle East, Central Asia, and Latin America. This Russian military intelligence-backed threat actor is actively involved in full-spectrum operations, such as espionage, attacks, and influence campaigns.

The group actively targets Critical Infrastructure and Key Resources (CIKR) operations worldwide, including in Poland, Kazakhstan, and Russia. APT44 has a history of disruptive actions, especially against Ukraine's energy sector. Using affiliated personas like the CARR, the group has claimed responsibility for manipulating industrial control systems (ICS) at water utilities and hydroelectric plants in the U.S. and Europe, such as Texas, Poland, and France. Additionally, APT44 regularly targets Western electoral systems and institutions to influence democratic processes globally, and conducts broad, less selective credential theft operations targeting mail servers in both the public and private sectors worldwide. They also frequently target journalists, civil society organizations, and investigative entities like the Organization for the Prohibition of Chemical Weapons (OPCW) and Bellingcat.

Intention(s)

APT44 conducts a comprehensive range of cyber attacks, espionage, and influence operations to support the Kremlin's geopolitical objectives and broad national interests. This full-spectrum approach exemplifies Russia's guiding concept of "information confrontation" (IPb). APT44's main goal is to function as a key strategic asset of power capable of addressing both ongoing and emerging intelligence needs, including efforts to disrupt democratic processes worldwide. The group targets espionage (KRIKS), attack (ITV), and influence (IPV).

Specifically, APT44's wartime aims focus on helping the Russian military achieve a tactical and operational advantage, with an increased emphasis on intelligence collection (espionage) to support conventional forces, such as exfiltrating encrypted communications from captured mobile devices. At the same time, APT44 is responsible for nearly all disruptive and destructive operations against Ukraine over the past decade, using tools like wiper malware to impact critical infrastructure sectors.

Beyond the conflict, the group's goal is to signal the seriousness of Russia's cyber threat and political dissatisfaction through cyber sabotage, such as disrupting the Pyeongchang Olympics or deploying NotPetya. Finally, APT44 intentionally participates in information operations by using front personas like CARR and Solntsepek to publicly claim credit, amplify disruption narratives, and cause second-order psychological effects, thereby trying to make GRU's cyber capabilities seem

more powerful. Ukraine is expected to remain the main focus of their operations as long as Russia's conflict persists.

TTP(s)

The Tactics, Techniques, and Procedures (TTPs) used by APT44 are adaptable and aggressive, reflecting its goal to carry out the full range of cyber espionage (KRIKS), attack (ITV), and influence operations (IPV). APT44 follows a highly flexible playbook designed to bypass best-practice defenses, emphasizing scalability and minimizing forensic evidence.

The methodology of APT44 generally adheres to five key phases of activity:

1. **Living on the Edge** (Initial Access)
2. **Living off the Land** (Reconnaissance, Lateral Movement)
3. **Going for the GPO** (Persistence, Privilege Escalation)
4. **Disrupt and Deny** (Attack/Sabotage)
5. **Telegraphing "Success"** (Influence, Information Operations)

Phase 1: Living on the Edge

TTP	Description
Exploitation of Edge Infrastructure	Frequently achieved through exploiting edge infrastructure, such as routers and VPN appliances. This establishes footholds used for subsequent reconnaissance or malware deployment
Phishing and Credential Harvesting	Uses common vectors like phishing and credential harvesting. Conducts widespread credential theft campaigns targeting public and private mail servers globally (Exim, Zimbra, Exchange) since at least 2019. Phishing campaigns may deliver droppers like PENNYBAG or HEXCHAMBER (A107-039)
Supply Chain Compromise	Subverting software supply chains for initial access, leading to downstream compromise of critical infrastructure networks in Eastern Europe and Central Asia

Trojanized Software/Opportunistic Access	Uses unconventional methods like distributing trojanized software installers via torrents on Ukrainian and Russian language forums for opportunistic access. They flag victims of interest manually after download for follow-on exploitation.
Vulnerability Exploitation	Exploits known vulnerabilities, such as a WinRAR vulnerability (CVE-2023-38831), to deliver dropper malware like SMOKELOADER, which then loads RADTHIEF infostealer.

Phase 2: Living off the Land

TTP	Description
Living Off the Land (LOTL)	Uses pre-existing tools and native OS commands (Windows net commands) for reconnaissance, lateral movement, establishing persistence, and information theft to evade detection. This includes abusing standard utilities like SDELETE and WinRAR to achieve disruptive objectives.
GPO Abuse for Persistence	Leveraging Group Policy Objects (GPO) to spread and deploy wipers ("Going for the GPO"). This involves utilities like TANKTRAP (a PowerShell script utilizing GPO to launch wipers like CADDYWIPER and SDELETE).
Scheduled Tasks	Establishing persistence using scheduled tasks (T1547, System Initialization Items). For example, via droppers like SHARPIVORY.
Lateral Movement	Uses tools like ITCHYSPARK (ITCHYSPARK.SM and ITCHYSPARK.WMI) for lateral movement to deploy wipers like NEARMISS.
Credential Dumping/Theft	Using the infostealer RADTHIEF (Rhadamanthys Stealer) to collect credentials. Credentials stored by browsers and FTP clients are targeted by DARKCRYSTALRAT.

Defense Evasion	Using techniques like T1027 (Detection Prevention/Obfuscation). Using modified publicly available tools and open-source tooling makes activity appear to be a commodity threat, aiding evasion. Custom malware is often lightweight and expendable.

Phase 3: Going for the GPO

TTP	Description
Custom Backdoors	Deploying custom backdoors like AXETERROR (Go-based backdoor that uses HTTPS and cron jobs for persistence), EARLYBLOOM (C++ backdoor communicating over HTTPS, EXARAMEL (backdoor encrypting and exfiltrating files), and QUICKTOW (lightweight Go-based HTTP backdoor).
Commody C2 Frameworks	Utilizes existing frameworks like DCRAT, EMPIRE (PowerShell post-exploitation framework), and METERPRETER (from METASPLOIT).
Web Shells	Uses web shells like BRUSHPASS (C# web shell for command execution/firewall modification) and publicly available web shells like WSO (PHP-based).
Tunnelers	Leveraging open-source tunnelers such as CHISEL, GOGETTER (Go-based tunneler using Yamux over TLS), and REGEORG.NEO (SOCKS proxy tunneler).

Phase 4: Disrupt and Deny

TTP	Description
Destructive Wiper Malware	Aggressively deploying wiper malware against civilian and military targets in Ukraine. Malware families include CADDYWIPER, NEARMISS, NEARTWIST, PARTYTICKET, JUNKMAIL, NIKOWIPER< ROARBAT (uses WinRAR to delete data), ETERNALPETYA (disguised as ransomware, and SOURGRAPES (OlympicDestroyer).
ISC/OT Disruptive Capabilities	Operating advanced capabilities intended to disrupt industrial control and safety systems, including the deployment of a new variant of Industroyer. They also use LOTL attack capabilities that abuse a native MicroSCADA binary.
Operational Coordination	Coordinating the timing of cyber attacks with conventional military activity (kinetic strikes or sabotage) to achieve joint military objectives in Ukraine.
Mobile Device Espionage	Provisioning infrastructure for Russian military forces to exfiltrate encrypted Telegram and Signal communications from mobile devices captured on the battlefield. This infrastructure includes step-by-step Russian instructions for linking chat applications (requires physical access).
Android Espionage	Operating "Infamous Chisel" to collect system and application data from Android devices, including applications specific to the Ukrainian military.
Disguised Ransomware/Wiper	Deployment of malware like PRESTEA (Prestige), which encrypts local files and uses wbadmin to delete backups, but is typically a disruptive tool signaling bilateral displeasure.

Phase 5: Telegraphing "Success"

TTP	Description
Hack-and-Leak / Attack-and-Leak	Primarily focuses on posting sensitive documents or "proof" of preceding cyber operations to Telegram channels (e.g., CyberArmyofRussia_Reborn, Solntsepek, XakNet Team) to draw attention to alleged impacts.
ICS/OT HMI Manipulation Claims	Associated hacktivist persona CARR claims to conduct Manipulation of ICS (T0831). These videos allegedly show manipulation of HMI at water utilities (US/Poland) and hydroelectric facilities (France). This manipulation may rely on simple access via unsecured VNC connections.
Amplification and Narrative Control	Amplifying the narrative of successful disruption, regardless of the actual impact, to generate support for Russia and make the GRU's capabilities appear more potent.
Distributed Denial of Service (DDoS)	Front personas like CARR and People's Cyber Army are known to use DDoS attacks (T1498). CARR uses botnets to achieve disruption. These groups may announce "training DDoS attacks" ahead of large events, such as the Paris Olympics.

APT44 mobilizes or directs affiliated hacktivist groups like CARR, Solntsepek, and XakNet Team, who use tools for large-scale DDoS attacks.

- **DDOSIA**: DDOSIA is a primary application used by the CARR-affiliated group NoName057(16). This tool performs denial-of-service attacks by sending persistent network requests based on instructions from a C2 configuration file. The tool supports HTTP, HTTP2, and TCP requests, and implementations exist in Python and Golang.

- **DDoS Botnets and Tools**: CARR employs large-scale DDoS attacks using botnets to overwhelm targeted networks. DDoS tools promulgated by the People's Cyber Army are coded in Python and feature multithreading, multiprocessing, and proxy support for Layer 4 and Layer 7 attacks.

- **Operational Technology (OT) Access**: The hacktivist front CARR claimed to manipulate ICS and human-machine interfaces (HMI) in the U.S. and Europe, possibly by simply accessing unsecured VNC connections.

- **BOBIK**: The BOBIK botnet (a remote access trojan) was used by NoName057(16) to carry out DDoS attacks.

Tool(s)/Malware

APT44 utilizes a diverse and adaptive arsenal of tools and malware to execute its full spectrum of operations, encompassing espionage, attack, and influence. The group's malware deployment strategy emphasizes a "low-equity" approach, frequently prioritizing open-source or commercially/criminally sourced tools over proprietary custom implants, especially for routine operations. When customizing, APT44 is known to create or modify lightweight, expendable tools to limit operational attrition, preferring to deploy its most advanced capabilities judiciously.

Generally, APT44 infiltrates victim systems using malicious software to install backdoors, often referred to as 'downloaders,' which grant persistence and allow the subsequent deployment of more potent payloads like information stealers or Remote Access Trojans (RATs). This approach relies heavily on LOTL techniques once inside a network, using pre-existing tools for reconnaissance, lateral movement, and information theft to aid detection evasion.

The malware used by APT44 falls into three categories: custom malware, modified publicly available tools, and readily available commercial/public tools. For its highly destructive and disruptive activities, APT44 employs a wide range of harmful malware, often referred to as wipers. Notable examples include the critical infrastructure framework INDUSTROYER, the infamous wiper disguised as ransomware, ETERNALPETYA (aka NotPetya), and modern wartime wipers like CADDYWIPER, NEARMISS, NIKOWIPER, JUNKMAIL, and PARTYTICKET. For tactical espionage and initial access, APT44 leverages commodity malware like DARKCRYSTALRAT (DCRAT) and tools such as SMOKELOADER and RADTHIEF (aka Rhadmanthys Stealer). The group increasingly abuses common utilities and publicly available software such as SDELETE (often embedded in wipers like NIKOWIPER) and WinRAR (used by the ROARBOAT wiper) to achieve disruptive goals, a strategy referred to as transitioning to "no equity" tooling.

Technical Information

Legend

1. Access & Persistence	
2. Staging & Delivery	
3. Execution & Utility	
4. Information Collection	
5. Destructive & Disruptive	

ID Labels

MITRE ATT&CK Technique label	T####
MITRE Software Label	S####
Vendor Canonical Label	VENDOR : TOOLNAME

Custom Wipers & Disruptive Tools

Malware	Role	ID	Description
CADDYWIPER	Wiper	S0693	Disruptive file wiper (written in C) that enumerates physical drives and overwrites file content and partitions with null bytes; has executable and shellcode variants. It was used alongside ARGUEPATCH in wiper attacks.

INDUSTROYER	Disruptive Malware Framework	S0604	Modular malware designed to survey and manipulate power grid control systems; includes modules to open/close circuit breakers, a wiper module, and a SIPROTEC DoS module. A new variant has been observed since Russia's re-invasion.
JUNKMAIL	Wiper	PALO ALTO NETWORKS : JUNKMAIL	A .NET wiper that overwrites files with null bytes after enumerating domain controllers, drives, directories, and files.
NEARMISS	Wiper	S0697	AKA HermeticWiper; MASTER BOOT Record (MBR) wiper; disables Shadow Volume Copy/CrashDumps, wipes the MBR, and initiates system shutdown.
NEARTWIST	Wiper	MANDIANT : NEARTWIST	Disruptive file wiper (written in C) that enumerates physical drives and attempts to wipe them using pseudorandom number generator data.
NIKOWIPER	Wiper	MANDIANT : NIKOWIPER	Diruptive tool (written in C) that embeds SysInternal's Sdelete executable to delete files on disk.
NIKOWIPER.MBR	Wiper	MANDIANT : NIKOWIPER.MBR	Same as NIKOWIPER, with additional functionality to wipe the MBR on victim devices.
PARTYTICKET	Wiper/Psuedo-Ransomware	MANDIANT : PARTYTICKET	Disruptive file wiper (written in Go) that encrypts file content with AES.
ROARBOAT	Wiper	MANDIANT : ROARBOAT	Batch disruptive wiper that enumerates drives/directories and uses WinRAR to delete data.

SOURGRAPES	Disruptive Malware	S0365	Destroys files on network shares and disables all services on a victim system (also known as OlympicDestroyer).

Custom Backdoors & Launchers

Malware	Role	ID	Description
ARGUEPATCH	Launcher	MANDIANT : ARGUEPATCH	Malicious launcher that decrypts a file on disk using trivial XOR and executes a second stage payload in memory. APT44 used this before dropping CADDYWIPER.
AXETERROR	Backdoor	ESET : AXETERROR	Backdoor (written in Go) that establishes persistence (cron job/startup script); communicates over HTTPS and supports shell commands and file transfers.
BACKORDER / BACKORDER V2	Downloader	MANDIANT : BACKORDER	Downloaders (written in Go) (Windows) that download and execute a second-stage payload. V2 can set %TEMP% as excluded from Windows Defender.
BRUSHPASS	Web Shell	MANDIANT : BRUSHPASS	Webshell (written in C#) used to execute commands, alter firewall configurations, and perform file management.
CHEMISTGAMES	Backdoor	MANDIANT : CHEMISTGAMES	A backdoor designed to provide remote acess and execute arbitrary commands on a compromised system.

COLDWELL	Dropper	MANDIANT : COLDWELL	Dropper (written in C) containing an encrypted payload; configured persistence and blends the next-stage timestamp.
EARLYBLOOM	Backdoor	MANDIANT : EARLYBLOOM	Backdoor (written in C++) that communicates over HTTPS; supports shell command execution and file transfer.
EXARAMEL	Backdoor	S0401 (Linux Variant) S0343 (Windows Variant)	Backdoor capable of encrypting and exfiltrating files, and executing commands received from C2 (configuration stored in XML in the registry).
FAIRROT	Dropper	ESET : FAIRROT	VBScript macro used to deliver an encoded payload; capable of sandbox detection.
FELIXROOT	Backdoor	S0267	Memory-only DLL backdoor used for reconnaissance, data exfiltration, and remote code execution; communications are AES-encrypted.
FIZZLESHELL	Web Shell	MANDIANT : FIZZLESHELL	PHP web shell employing cryptography to obfuscate commands; communiocates sent to hardcoded C2 server via MIME message in HTTP(S) POST data.
FREETOW	Memory-Only Dropper	MANDIANT : FREETOW	In-memory dropper for shellcode payload, identified as a payload patched into legitamate Microsoft applications.
GREYENERGY	Backdoor	S0342	Backdoor framework used for espionage and reconnaissance, considered a successor to BlackEnergy.

ICYWELL	Backdoor	MANDIANT : ICYWELL	Backdoor (written in C++) that provides a reverse shell and executes arbitrary commands.
ILLICITORDER	Backdoor	MICROSOFT : ILLICITORDER	Dropper (written in C++) containing an XOR and Base64-encoded payload; embedded into trojanized software installation media.
KAPEKA	Backdoor	MICROSOFT : KAPEKA	Backdoor with a flexible framework that allows APT44 to deploy additional modules on compromised systems.
LUCKYPIE	Launcher	MANDIANT LUCKYPIE	Loads and executes a DLL from its resourece section; embedded into the zlib library code.
NEWRETURN	Memory-Only Dropper	ESET : NEWRETURN	In-memory .Net dropper containing an embedded binary that is decompressed and executed.
QUICKTOW	Backdoor	MANDIANT : QUICKTOW	Lightweight backdoor (written in Go); communicates via HTTP; can connect to other instances to forward commands.
SHARPCOFFEE / SHARPCOFFEE.VBS	Downloader	MANDIANT : SHARPCOFFEE	SHARPCOFFEE (JavaScript) and SHARPCOFFE>VBS (Visual Basic) downloaders retrieve payloads (the former executes via PowerShell sub-process).
SHARPENTRY	Downloader	MANDIANT : SHARPENTRY	Downloader (written in C); retrieves TCP payloads, which are decoded and mapped into memory; observed deploying METERPRETER.

SHARPIVORY	Dropper	MANDIANT : SHARPIVORY	.NET dropper that establishes persistence via scheduled tasks and drops a decoy Microsoft Office Word document.
SPAREPART	Backdoor	MANDIANT : SPAREPART	Lightweight backdoor (written in C) that uses the device's UUID for C2 communications.
SWEETTREAT	Utility	MANDIANT : SWEETTREAT	Utility service providing crpytographic functionality via named pipe or RPC.
VPNFILTER	Backdoor	S1010	Modular backdoor entensible through plugins.

Modified Public or Commercially Available

Malware	Role	ID	Description
BLACKENERGY	Backdoor	S0089	Early variants were DDoS botnets; V2 and V3 modular backdoors were utilized by APT44 specifically for espionage
ETERNALPETYA	Wiper/Pseudo-Ransomware	S0368 (NotPetya)	A destructive tool (aka NotPetya) disguised as ransomeware, capable of encrypting files/MBR, installing a bootkit, extracting credentials, and performing remot exploitation.
HEXCHAMBER	Builder	MANDIANT : HEXCHAMBER	Custom implementation of the open-source Malicious Macro Generator (MMG) project, used to distribute PowerShell Empire.

KillDisk	Wiper	S0139	A destructive malware component designed to overwrite and erase data from disk drives, rendering systems inoperable.
POWERDISCO	Utility	ESET : POWERDISCO	Modified Windows PowerShell script used to enumerate Group Policy Objects (GPO) via ADSI.
TANKTRAP	Utility	MANDIANT : TANKTRAP	PowerShell utility that uses Windows Group Policy to spread and launch wipers such as NEARMISS, SDELETE, PARTYTICKET, and CADDYWIPER
WILDDIME	Backdoor	MANDIANT : WILDDIME	Modified PowerShell backdoor (variant of the public HTTP-Shell tool) capabile of file transfer and execution

Publicly or Commercially Available Tools and Capabilities

Malware	Role	ID	Description
Impacket	Utility	S0357	Open-source collection of Python scripts used for network protocol manipulation, available to anyone on GiTHub
Invoke-PSImage	Dropper	PowerSploit : Invoke-PSImage	Open-source PowerShell script that is part of the PowerSPloit post-exploitation framework.
SDELETE	Utility/Wiper	S0195	A common utility abused for disruptive objectives. Embedded in NIKOWIPER.

WinRAR	Utility/Wiper	T1560 & T1204	Abused for destructive ojectives (used by ROARBAT). Exploiting a WinRAR vulnerability (CVE-2023-38831) was used to deliver SMOKELOADER.
MicroSCADA binary	Utility/LOTL	HITACHI ENERGY : MICROSADA	Native binary abused for OT-specific LOTL attacks.

Espionage & Info Stealers

Malware	Role	ID	Description
Mimikatz	Info Stealer	S002	Post-exploitation tool used to extract plaintext passwords, hashes, and Kerberos tickets from history.
Infamous Chisel	Info Stealer	CISA: INFAMOUS CHISEL	Tool used to collect information from Android devices, including system data and details from applications specific to the Ukrainian military.
RADTHIEF	Info Stealer	MCAFEE : RADTHIEF	Known as "Rhadamanthys Stealer," it collects credentials, system information, browser data, and crypto wallet data. Delivered via SMOKELOADER.

DARKCRYSTALRAT (DCRAT)	Backdoor	SPLUNK : DARKCRYSTALRAT	.NET-based backdoor providing remote desktop, file transfer, shell execution, and credential theft (browsers/FTP clients).

Frameworks & Backdoors

Malware	Role	ID	Description
BEACON	Backdoor	S0363	Component of the Colbalt Strike framework
COBALT STRIKE	Framework	S0154	A commercial adversary simulation tool widely abused by APT44 for post-exploitation and lateral movement.
CYCLOPS BLINK	Framework	S0649	Malware framework developed and used exclusively by APT44 as a replacement for VPNFilter.
EMPIRE	Framework	S0363	PowerShell post-exploitation framework.
EMPYRE	Framework	S0325	OS X/Linux pen-testing framework inspired by PowerShell Empire.
METASPLOIT / METERPRETER	Framework/Backdoor	S0012	Penetration testing framework used to generate the METERPRETER backdoor. APT44 also uses the Python implementation, METERPRETER.PYTHON
PASWEB	Web Shell	S0598	Publicly available P.A.S. PHP web shell
STOWAWAY	Backdoor/Proxy	DFIR-GO : STOWAWAY	Publicly available backdoor and proxy supporting remote shell and file management.

WARZONE	Backdoor	Uptycs : WARZONE RAT	Backdoor (written in C++) with capabilities including video/screenshot capture, remote desktop, keylogging, and credential extraction.
WEEVELY	Web Shell	EPINNA : WEEVELY	Open-source, small, polymorphic PHP webshell extensible over the network at runtime.
WSO	Web Shell	ORB : WSO	PHP-based webshell backdoor requiring a password to operate.

Downloaders & Tunnelers

Malware	Role	ID	Description
COLIBRI	Downloader	BITSIGHT : COLIBRI	Evasive, obfuscated C++ Win32 downloader that executes implants in-memory.
SMOKELOADER	Downloader	S0226	Retrieves and maps additional payloads into memory; functionality includes keylogging, credential theft, and DDoS via plugins. Used to deliver RADTHIEF.
CHISEL	Tunneler	JPILLORA : CHISEL	Open-source tunneler relied on more heavily as the war progressed.
GOGETTER	Tunneler	MANDIANT : GOGETTER	Written in Go; proxies C2 communications using Yamux over TLS
PIVOTNACCI	Tunneler	BLACKARROWSEC : PIVOTNACCI	Open-source tunneler that deploys HTTP agents to pivot into internal networks via SOCKS server.

REGEORG / REGEORG.NEO	Tunneler	S1187 (reGeorge) S1189 (Neo-reGeorge)	Open-source utilities used to tunnel webshell traffic, with REGEORG.NEO being a refactored fork that tunnels via SOCKS proxies.

Other Utilities/Exploits

Malware	Role	ID	Description
REMCOM	Utility	INTELLIADMIN : REMCOM	Lateral movement tool that reimplements the logic of Sysinternals PsExec.
PWNKIT	Exploit	CVE-2021-4034	Implementation of CVE-2021-4034 used for privilege escalation
WMIEXEC	Backdoor	SecureAuth : Impacket	Lightweight VBScript backdoor utilizing WMI to execute shell commands or createa reverse shell.
AcidPour	Wiper	S1167	Novel malware that may have been used in telecommunications attacks against ISPs; compiled for a wide range of Linux systems and shares wiping functionalities with AcidRain
AcidRain	Wiper	S1125	AcidRain is a malware that was used to target Viasat and shares equivalent wiping functionalities with the AcidPour malware.
POEMGATE	PAM Module	MANDIANT : POEMGATE	Malicious PAM module discovered on compromised Linux servers during the Kyivstar attack, allowing authentication with a statically defined password.

WhiteCat Log Cleaner	Utility	MANDIANT : WHITE CAT LOG CLEANER	Leveeraged to clear various log files, such as access or error logs, to remove evidence of unauthorized activity.
FrostyGoop	Malware	S1165	Novel malware (written in Golang) designed to target OT via the Modbus protocol, discovered during the attack planning against Ukrainian energy entities.

Assessment

Advanced Persistent Threat 44 (APT44), also known as Sandworm, is a Russian GRU state-sponsored group conducting a full spectrum of ***cyber espionage, destructive attacks, and influence operations***. Active for **the past decade**, APT44's ***primary focus is Ukraine, but it maintains a global mandate, targeting government, defense, and critical infrastructure in North America and Europe***. The group is expected to continue these operations to *support the Kremlin's geopolitical objectives, provide tactical advantage for the Russian military, and undermine democratic processes worldwide*. *They typically gain access by exploiting edge infrastructure and using phishing, then move laterally using LOTL techniques before deploying destructive wipers like CADDYWIPER and ETERNALPETYA (NotPetya).* If defenses are not adapted, APT44 will remain a persistent, high-severity global threat designed to bypass best practice defenses and amplify the psychological impact of its attacks using front personas like CARR. Possible solutions include patching edge infrastructure, segmenting IT and OT networks, and deploying EDR solutions to detect their LOTL-based TTPs.

Legend: **Who**, ***What***, **When**, ***Where***, *Why*, *How*, So What?!, possible Solution

Source(s)

Anna Ribeiro (2025). Mandiant exposes APT44, Russia's Sandworm cyber sabotage unit, targeting global critical infrastructure. Industrial Cyber. https://industrialcyber.co/ransomware/mandiant-exposes-apt44-russias-sandworm-cyber-sabotage-unit-targeting-global-critical-infrastructure/

Ben McCarthy, Ben Hopkins (2025). ZEROLOT Analysis: Inside Sandworm's Destructive New Wiper. Immersive Labs. https://www.immersivelabs.com/resources/blog/zerolot-analysis-inside-sandworms-destructive-new-wiper

Christian Vasquez, AJ Vicens (Undated). Mandiant: Notorious Russian hacking unit linked to breach of Texas water facility. CyberScoop. https://cyberscoop.com/sandworm-apt44-texas-water-facility/

Council on Foreign Relations (Undated). Sandworm. CFR Interactives / Cyber Operations Tracker. https://www.cfr.org/cyber-operations/sandworm

Cyble (2025). People's Cyber Army & HackNeT Trial DDoS Attacks On France. Cyble Blog. https://cyble.com/blog/hacktivist-groups-peoples-cyber-army-and-hacknet-launch-trial-ddos-attacks-on-french-websites-prior-to-the-onslaught-during-paris-olympics/

Cyble (2025). Peoples Cyber Army Of Russia | Threat Actor Profile. Cyble. https://cyble.com/threat-actor-profiles/peoples-cyber-army-of-russia/

Daryna Antoniuk (2025). Russian hackers infiltrated Ukrainian telecom giant months before cyberattack. The Record from Recorded Future News.

Daryna Antoniuk (2025). Russian hackers turn to AI as old tactics fail, Ukrainian CERT says. The Record Media. https://therecord.media/russian-hackers-turn-to-ai-ukraine-cert

Daryna Antoniuk (2025). Sandworm APT Attacks Detection: Russian State-Sponsored Hackers Deploy Malicious Windows KMS Activators to Target Ukraine. SOC Prime. https://socprime.com/blog/detect-sandworm-apt-attacks-against-ukraine/

Directorate of Cyber Security Analysis, National Cyber Security Authority (2023). PROFILE OF RUSSIAN HACKER GROUPS. National Cyber Security Authority / Directorate of Cyber Security Analysis. https://aksk.gov.al/wp-content/uploads/2024/12/Profile-of-Russian-Hacker-Groups.pdf

Dragos Threat Intelligence; Hakan KARABACAK (2024). Sandworm Team. MITRE ATT&CK. https://attack.mitre.org/groups/G0034/

Eduard Kovacs (2025). Recent OT and Espionage Attacks Linked to Russia's Sandworm, Now Named APT44. SecurityWeek. https://www.securityweek.com/recent-ot-and-espionage-attacks-linked-to-russias-sandworm-now-named-apt44/

Gabby Roncone, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Dan Perez, Lexie Aytes, Alden Wahlstrom (2024). APT44: Unearthing Sandworm. Mandiant / Google Cloud. https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

Gabby Roncone, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Luke Jenkins, Dan Perez, Lexie Aytes, Alden Wahlstrom (2024). Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm

Jordyn Alger (2025). Russian Offensive Cyber Operations Analyzing Putin's Foreign Policy Actions. Security Magazine. https://www.securitymagazine.com/articles/101903-russian-offensive-cyber-operations-analyzing-putins-foreign-policy-actions

Mandiant Intelligence (2022). Hacktivists Collaborate with GRU-sponsored Threat Actors. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

Pawel Knapczyk, Nikita Kazymirskyi (2025). The Russia-Ukraine Cyber War Part 1: Three Years of Cyber Warfare. Trustwave SpiderLabs Blog. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/three-years-of-cyber-warfare-how-digital-attacks-have-shaped-the-russia-ukraine-war/

Pawel Knapczyk, Nikita Kazymirskyi (2025). The Russia-Ukraine Cyber War Part 2: Attacks Against Government Entities, Defense Sector, and Human Targets. Trustwave SpiderLabs Blog. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacks-against-government-entities-defense-sector-and-human-targets/

Pawel Knapczyk and Nikita Kazymirskyi (2025). The Russia-Ukraine Cyber War Part 3: Attacks on Telecom and Critical Infrastructure. Trustwave SpiderLabs Blog. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-russia-ukraine-cyber-war-part-3-attacks-on-telecom-and-critical-infrastructure/

Pawel Knapczyk and Nikita Kazymirskyi (2025). The Russia-Ukraine Cyber War Part 4: Development in Group Attributions for Russian State Actors. Trustwave SpiderLabs Blog. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/russian-state-actors-development-in-group-attributions/

Ravie Lakshmanan (2025). Microsoft Uncovers Sandworm Subgroup's Global Cyber Attacks Spanning 15+ Countries. The Hacker News. https://thehackernews.com/2025/02/microsoft-uncovers-sandworm-subgroups.html

Seth G. Jones (2025). Russia's Shadow War Against the West. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/russias-shadow-war-against-west

SOCRadar (2025). Dark Web Profile: Cyber Army of Russia Reborn. SOCRadar® Cyber Intelligence Inc. https://socradar.io/dark-web-profile-cyber-army-of-russia-reborn/

ThreatMon (2024). APT44: The Famous Sandworm of Russia. ThreatMon Blog. https://threatmon.io/apt44-the-famous-sandworm-of-russia/

ThreatMon (N/D). Understanding the 'KAPEKA' Backdoor: Detailed Analysis by APT44. ThreatMon. https://threatmon.io/understanding-the-kapeka-backdoor-detailed-analysis-by-apt44/

U.S. Department of the Treasury (2025). Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn. Press Release / News. https://home.treasury.gov/news/press-releases/jy2473