ORION FORUM

# APT Profile: APT44

AUGUST 25, 2026

| | |
|---|---|
| **Country of Origin** | Russia |
| **Threat Actor Type** | State-sponsored |
| **Other Names** | Sandworm, GRU Unit 74455, Seashell Blizzard, FROZENBARENTS Iron Viking, Telebots, Voodoo Bear |
| **Year Identified** | 2014 |
| **Major Target Countries & Entities** | Ukraine, Poland, United States, South Korea, multinational corporations |

## Profile Summary

APT44 is a Russian state-sponsored cyber threat actor that operates within a specialized unit of the GRU (*Glavnoye Razvedyvatelnoye Upravleniye*), Russia's military intelligence agency. Its core mission combines cyber espionage operations with physically disruptive and destructive cyberattacks. It is one of the few known groups to have caused kinetic effects with cyber operations, and it has also been involved in influence and informational operations and has been suspected to be responsible for election disruptions. APT44 operates under the Main Centre for Special Technologies (GTsST) in the GRU, and has primarily provided support for the Russian military's operations against Ukraine. Google's cybersecurity subsidiary Mandiant designated the group as an Advanced Persistent Threat in 2024.

APT44 first formed in 2009 but was not publicly identified until 2014. As a state-affiliated group, APT44's major operations have aimed to directly support Russian political objectives, primarily the invasion of Crimea in 2015 and the ongoing conflict between Russia and Ukraine.

The most significant operations attributed to APT44 include an attack on a Ukrainian power grid in 2015, leading to outages for 230,000 people; installation of wiper software on hundreds of Ukrainian companies' systems using stolen NSA technology in 2017; and disruption of the opening ceremony of the 2018 Olympic Games using malware designed with a nearly identical fingerprint to a North Korean hacker group. Six GRU officers in APT44 were indicted for these attacks in October of 2020, and the U.S. Attorney General for National Security John C. Demers stated that "No country has weaponized its cyber capabilities as maliciously and irresponsibly as Russia, wantonly causing unprecedented collateral damage to pursue small tactical advantages and to satisfy fits of spite." U.S. Attorney Scott W. Brady for the Western District of Pennsylvania stated that APT44 was responsible for "the most destructive and costly cyber-attacks in history." The identities of the other members of APT44, the number of people contributing to its operations, and the full scale of its capabilities remain largely unknown. APT44 remains one of the world's most destructive state-sponsored cyber units, executing sophisticated operations with massive impact and demonstrating the unique capability to extend them far past the digital realm.

**Background and Development**

In 2014, researchers were able to identify APT44 as a distinct group through its repeated use of BlackEnergy malware to conduct spearphishing and reconnaissance operations. This kind of malware is used to gain access to industrial control systems through human-machine interfaces, and is typically delivered through spear-phishing emails. The group's first known activity used this malware to extract data from Ukrainian and NATO member states' government networks. Later that year, they launched a large-scale DDoS (Distributed Denial of Service) attack on Ukrainian communications networks during the invasion of Crimea. The name "Sandworm" came from these early malware samples analyzed by researchers, and references a character in Frank Herbert's novel Dune. APT44 also frequently collaborates with some of the GRU's other well-known cyber units, such as APT28 (Unit 26165/FancyBear) during an operation targeting the 2017 French presidential election.

From 2009 to 2022, the group's activities were very broad in scope. While most Russian state-sponsored groups specialized in a single type of operation, APT44's activities have been

unusually dynamic, covering a wide range of espionage, attack, and influence operations. These were primarily aimed at supporting Russian state military objectives, though these activities ranged from disrupting private firms' communication networks in Ukraine during an invasion to disrupting the Olympics opening ceremony after Russia was banned from the Games that year. After 2022, APT44 transitioned to a more military-oriented approach, more aggressively targeting Ukraine and its allies since the start of the war to help the Kremlin gain an advantage. Their operations are also frequently more directly integrated with conventional military operations. For example, in October of 2022, APT44 disrupted the IT and OT systems of a power distribution center in Ukraine while armed forces targeted the energy grid with missile and drone strikes.

### Organizational Structure and State Affiliation

While APT44 officially operates as a unit under the jurisdiction of the GRU, very little is known about its structure and leadership. It is suspected to operate under the oversight of the GRU's Information Operation Troops (also known as VIO or Unit 55111). The designation of the group as an APT, however, and the name APT44, refers to a set of individuals and their cyber activity as a collective as it is observed by external governments, researchers, and security firms.

The clearest information about APT44's structure emerged from the 2020 indictment of six GRU officers confirmed to be affiliated with the group. They were charged for their involvement in several major APT44 operations, though their exact roles were not disclosed. GRU Colonel Yevgeny Mikhailovich Serebriakov, who was also indicted in 2018 for his involvement in several major GRU-attributed cyber operations, was allegedly placed in a leadership position within APT44's GRU unit around 2022. Unit 74455 officially operates out of Khimki, near Moscow, but it is unknown whether members of the group are actually located there. They are known to sometimes collaborate with other Russian cyber actors, such as APT28/Fancy Bear, though they have a greater focus on cyber-kinetic operations rather than just intelligence collection and cyber espionage. The GRU is also known to actively recruit students from top Russian universities for their cyber units.

The Russian government is linked to a broad network of cyber groups and maintains different levels of control over each. Some are directly state-sponsored, like APT44, while others are hacktivist organizations that receive support from the government or even criminal groups that have developed working relationships with the GRU. APT44 is thought to be the most deeply integrated with the state, directly supporting military objectives and frequently working in tandem with the armed forces' conventional operations.

## Strategic Objectives and Target Profile

APT44 is the only Russian state-sponsored group to engage in cyber espionage, cyberattacks, and information or psychological influence, rather than specializing in one particular type of operation. In operations extending far beyond the Kremlin's aims in Ukraine, APT44 has targeted the electoral systems of current or prospective NATO states. The group has used malware to interfere with electronic voting systems, misrepresent data, and leak sensitive information. APT44 frequently gains access to systems of both governments and private firms using spearphishing campaigns, supply chain compromises, and living-off-the-land techniques (using tools within a pre-existing system to carry out an attack). It then uses malware families such as NotPetya, Industroyer, or BlackEnergy to disrupt or directly manipulate systems and delete data. The group has also been known to utilize "hacktivist" personas and false-flag operations, replicating other cyber actors' malware fingerprints to avoid identification.

Because APT44 operates as a unit of the Russian military, its attacks primarily aim to support Russian geopolitical objectives and government agencies, critical infrastructure, and private firms make up the vast majority of its targets. Other entities that have been attacked by APT44 include telecommunications and media, higher education, and research institutions. Those within Ukraine are most frequently targeted, as well as in NATO and EU member states. Operations have previously been conducted in many countries, including Azerbaijan, Belarus, Denmark, France, Georgia, Iran, Israel, Kazakhstan, Kyrgyzstan, Lithuania, Poland, Russia, South Korea, the United States, and Ukraine. Frequently-targeted sectors include energy, government, telecommunications, media, civil society organizations, and defense.

## Attribution and Evidence

Responsibility for major attacks has primarily been attributed to APT44 through frequent reuse of particular custom malware families, operations coinciding with Russian military offensives, and targeting that aligns with Russia's broader strategic or ideological aims (such as the attack on the Olympic Games' broadcasting systems after Russia was banned from competing). The group is also well known for using various personas to publicly take credit for cyber attacks, data leaks, and other disruptive actions. These personas are typically hacktivist organizations, promoting pro-Russian ideologies across various Telegram channels and other online platforms, which allows APT44 to maintain plausible deniability and conceal their direct link to the state.

APT44 is also known for employing a diverse range of methods for initial access to digital systems, including spear-phishing, vulnerability exploitation, and supply chain compromise. It frequently targets infrastructure such as routers, human-machine interfaces, and VPNs to gain initial access and deploy malware. It also frequently uses living-off-the-land techniques to avoid detection and maintain access to these systems for extended periods of time before conducting an attack. These particular behaviors, as well as "fingerprints" in their malware, allow government organizations and private cybersecurity firms to identify APT44's activities, though the group has also been known to replicate the fingerprints of other widely-known cyber threat groups.

**Impact Assessment**

APT44's full capabilities remain largely unknown. It also remains unclear whether, or to what extent, APT44 has access to critical infrastructure networks within the United States, and how long they remain within a compromised network before launching an attack. It is more deeply integrated with Russia's armed forces than it has ever been, and as a result, it has played a pivotal role in supporting conventional operations in Ukraine. While it is still deeply integrated with the armed forces, APT44's focus on Ukraine has recently shifted from disruption to reconnaissance and intelligence collection. Its primary aim is to give the military a battlefield advantage by disrupting Ukraine's operations. While its outer layers and some specific malware the group uses are well-documented, the internal dynamics of the group, how it operates with Kremlin leadership, and the full scope of its capabilities are largely unknown.

APT44's most well-known attack was a massive campaign that impacted hundreds of firms around the world, including several multi-billion-dollar corporations. This was known as the "NotPetya" attack, which encrypted data and disabled networks within these companies and halted global supply chains by targeting Maersk, impacting nearly a fifth of the world's shipping capacity. The attack utilized malware called EternalBlue that had been stolen from the U.S. National Security Agency in 2017 and Mimikatz, malware that had been created by a French researcher in 2011. It aimed to find a vulnerability in Windows systems, and it was initially deployed through M.E.Doc, software used to file taxes that was used by about 80% of Ukrainian businesses as well as Maersk. By combining two powerful malware packages, NotPetya could then spread across networks across the world within minutes, including Maersk's systems, and destroy data. 17 of Maersk's 76 international ports were affected, as well as Merck, TNT Express, and other global firms. The attack caused an estimated $10 billion, according to a White House assessment.

In December of 2025, Amazon Threat Intelligence reported that it had identified a campaign conducted between 2021 and 2025 targeting American and European critical infrastructure. It was linked with high confidence to APT44 and primarily targeted the energy sector. This activity continued into January 2026, when both Amazon and Microsoft reported sustained targeting of critical infrastructure through misconfigured network edge devices, VPNs, and collaboration platforms across North America and Europe. Amazon also reported a notable evolution in APT44's operations: attackers initially exploited zero-days in IT and network security systems such as WatchGuard Firebox, Atlassian Confluence, and Veeam. In 2025, they shifted to targeting misconfigured, publicly exposed edge devices—hardware components that act as data sources for a network, such as laptops and routers—rather than new vulnerabilities and less frequent zero-day vulnerability exploitation..

Around the same time the Amazon Threat Intelligence report was published, a collection of federal agencies including CISA, FBI, and NSA and global partners issued a joint Cybersecurity Advisory on pro-Russia hacktivist groups, including APT44-linked personas, conducting opportunistic attacks on U.S. critical infrastructure. The warning stated that these Russian-affiliated groups are actively targeting U.S. and global critical infrastructure across several

sectors, exploiting known vulnerabilities rather than pursuing strategically selected targets. These attacks, while less sophisticated than those conducted by APTs, are still able to access critical infrastructure and cause physical damage, exploiting virtual network computing connections to access operational technology. This advisory also stated that APT44 is also likely responsible for supporting the creation of CARR (also known as the “Cyber Army of Russia Reborn”) beginning in early 2022. This group has claimed several DDoS attacks against the U.S. and Europe for supporting Ukraine, spreading pro-Russian rhetoric online, and conducting attacks on industrial control systems in a wastewater treatment facility in Europe and human-machine interface devices at a U.S. farm in 2023. Since these operations, CARR is believed to be operating alongside the Russian government. A portion of its leadership, dissatisfied with GRU support and funding, left the group to form Z-Pentest, another cyber threat group separate from the GRU.

APT44 poses a significant risk to U.S. national security not solely as an individual threat actor, but as a proliferation risk for new cyber tactics, which could lower the barrier of entry for state and non-state groups to develop their own operations. It is also one of the only groups that has caused physical disruptions through cyber attacks by using sophisticated cyber intrusion techniques for attacks on critical systems such as power grids. Given APT44’s history of interfering in democratic processes, its threat potential is elevated as pivotal elections in the coming years are set to shape the trajectory of Western military aid to Ukraine. Organizations worldwide risk falling into the group’s sights as these elections draw closer.

### Major Cyber Operations

| Date | Operation / Target | Attack Type | Sector | Impact |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| March – December 2025 *(attributed to Sandworm with medium confidence due to overlap with previous APT44 wiper attacks)* | Wind farms, solar farms, power plant in Poland | Wiper malware ( DynoWiper) | Energy | The atta distribu resourc disrupt generat interrup commu betwee the syst Over 30 targete |
| April 2022 | Ukrainian power grid | Industroyer malware with false flags to disguise it as Lazarus Group (DPRK) malware | Energy | Planned widespr but was Ukrainia |
| 9 February 2018 | 2018 Olympic Games broadcasting (wi-fi and TV networks) | Wiper malware | IT infrastructure, telecommunications | Disrupti TV netw Pyeongc Stadium Olympic security were ab essentia but the to be re |

| | | | | |
|---|---|---|---|---|
| June 2017 | Initially targeted accounting systems within Ukrainian companies, then spread to major global firms including shipping, pharmaceuticals, and consumer goods. | NotPetya malware: a combination of EternalBlue (stolen from the NSA) and Mimikatz (created by a French researcher in 2017).<br><br>This combination of malware was particularly damaging because it did not require direct human interaction, allowing it to spread across networks and destroy massive amounts of data in seconds. | Financial systems, government agencies, critical infrastructure. Reached multinational corporations and disrupted global supply chains. | Became “NotPet and cau billion in disrupte supply c attacks Merck, a major c Irrevers and des paralyz infrastru corpora governn |

| | | | | |
|---|---|---|---|---|
| 17 December 2016 | Power grid in Kyiv | Industroyer, CRASHOVERRIDE malware; Exploited vulnerability in protective relays | Energy | Disrupte power g 20% of power f The US Dragos the atta to dama equipm have be safety r enginee restore |
| 23 December 2015 | Ukrainian power grid | BlackEnergy 3 malware | Energy | Disrupte for as m 230,000 Ukraine hours. |