Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm

By Mandiant

Published: 2024-04-17 · Archived: 2026-04-05 14:19:40 UTC

Written by: Gabby Roncone, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Luke Jenkins, Dan Perez, Lexie Aytes, Alden Wahlstrom

---

With Russia's full-scale invasion in its third year, Sandworm (aka FROZENBARENTS) remains a formidable threat to Ukraine. The group's operations in support of Moscow's war aims have proven tactically and operationally adaptable, and as of today, appear to be better integrated with the activities of Russia's conventional forces than in any other previous phase of the conflict. To date, no other Russian government-backed cyber group has played a more central role in shaping and supporting Russia's military campaign.

Yet the threat posed by Sandworm is far from limited to Ukraine. Mandiant continues to see operations from the group that are global in scope in key political, military, and economic hotspots for Russia. Additionally, with a record number of people participating in national elections in 2024, Sandworm's history of attempting to interfere in democratic processes further elevates the severity of the threat the group may pose in the near-term.

Given the active and diffuse nature of the threat posed by Sandworm globally, Mandiant has decided to graduate the group into a named Advanced Persistent Threat: **APT44**. As part of this process, we are releasing a report, "APT44: Unearthing Sandworm", that provides additional insights into the group's new operations, retrospective insights, and context on how the group is adjusting to support Moscow's war aims.

Key Findings

Sponsored by Russian military intelligence, APT44 is a dynamic and operationally mature threat actor that is actively engaged in the full spectrum of espionage, attack, and influence operations. While most state-backed threat groups tend to specialize in a specific mission such as collecting intelligence, sabotaging networks, or conducting information operations, APT44 stands apart in how it has honed each of these capabilities and sought to integrate them into a unified playbook over time. Each of these respective components, and APT44's efforts to blend them for combined effect, are foundational to Russia's guiding "information confrontation" concept for cyber warfare.

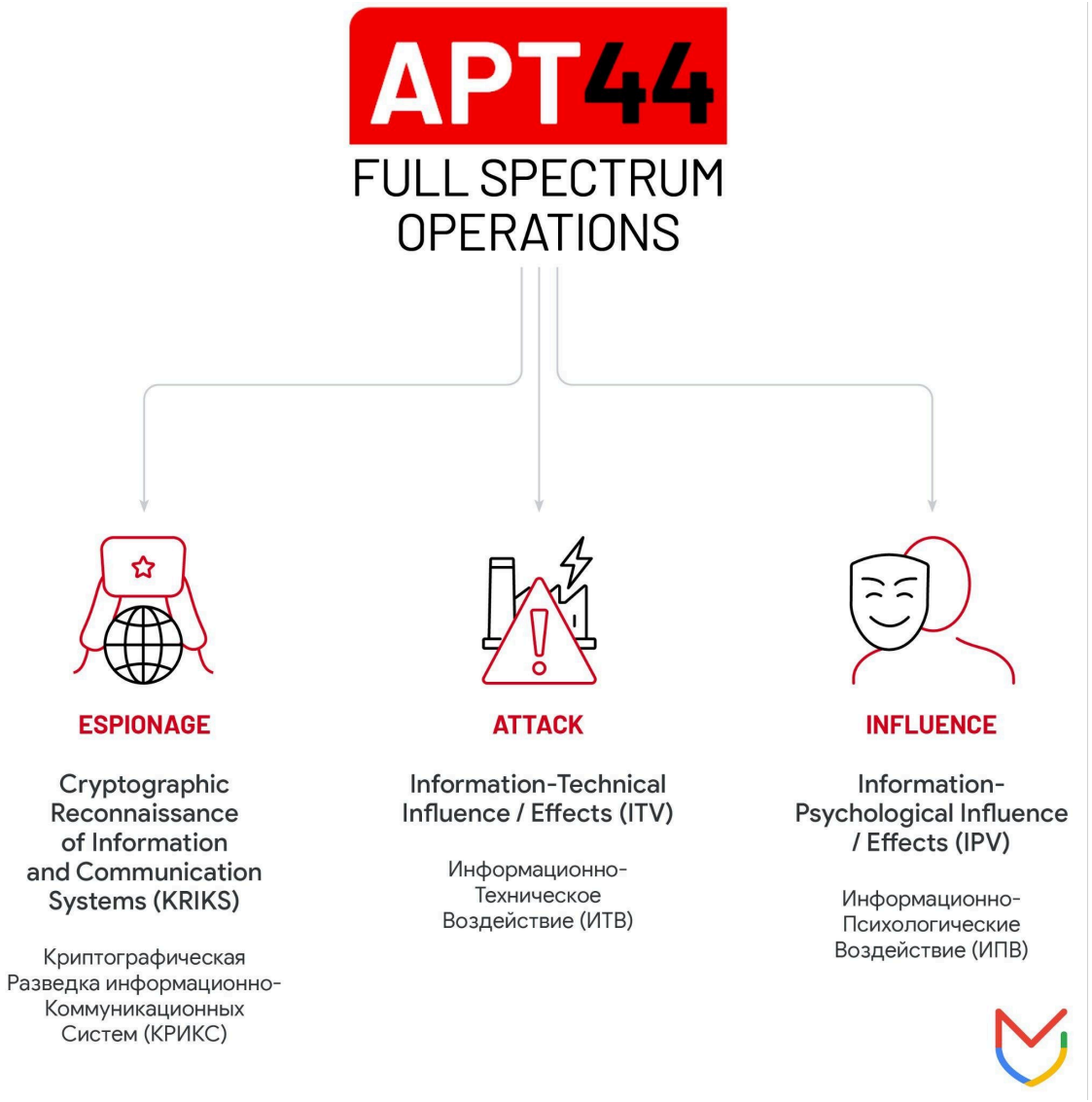

Figure 1: APT44's spectrum of operations

APT44 has aggressively pursued a multi-pronged effort to help the Russian military gain a wartime advantage and is responsible for nearly all of the disruptive and destructive operations against Ukraine over the past decade. Throughout Russia's war, APT44 has waged a high intensity campaign of cyber sabotage inside of Ukraine. Through the use of disruptive cyber tools, such as wiper malware designed to disrupt systems, APT44 has sought to impact a wide range of critical infrastructure sectors. At times, these operations have been coordinated with conventional military activity, such as kinetic strikes or other forms of sabotage, in an attempt to achieve joint military objectives.

However, as the war has endured, APT44's relative focus has transitioned away from disruption to intelligence collection. The group's targets and methods have shifted significantly in the second year of the war, with increasing emphasis placed on espionage activity intended to provide battlefield advantage to Russia's conventional forces. For example, one long-running APT44 campaign has assisted forward-deployed Russian ground forces to exfiltrate communications from captured mobile devices in order to collect and process relevant targeting data. APT44's approach to supporting Russia's military campaign has evolved considerably over the past two years.

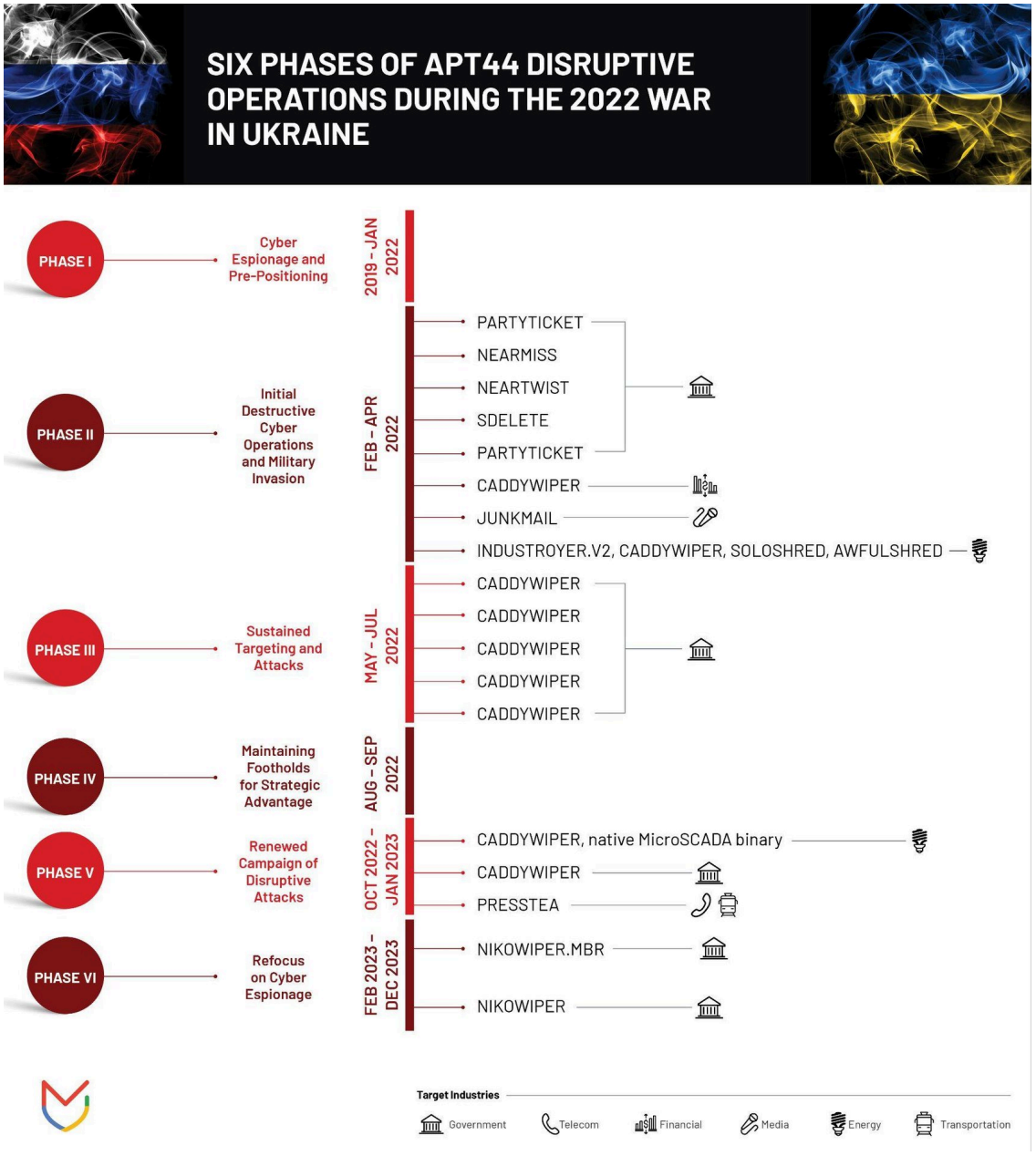

Figure 2: APT44’s wartime disruptive activity

We assess with high confidence that APT44 is seen by the Kremlin as a flexible instrument of power capable of servicing Russia's wide ranging national interests and ambitions, including efforts to undermine democratic processes globally.

Despite being an arm of Russia’s military, the group’s sabotage activity is not limited to military objectives and also spans Russia’s wider national interests, such as driving the Kremlin’s political signaling efforts, responses to crises, or intended non-escalatory responses to perceived slights to Moscow’s stature in the world.

APT44’s support of the Kremlin’s political objectives has resulted in some of the largest and most consequential cyber attacks in history. These operations include first-of-their-kind disruptions of Ukraine's energy grid in the winters of 2015 and 2016, the global NotPetya attack timed to coincide with Ukraine’s Constitution Day in 2017,

and the disruption of the opening ceremony of the 2018 Pyeongchang Olympics in response to Russia's doping ban from the games, to name a few.

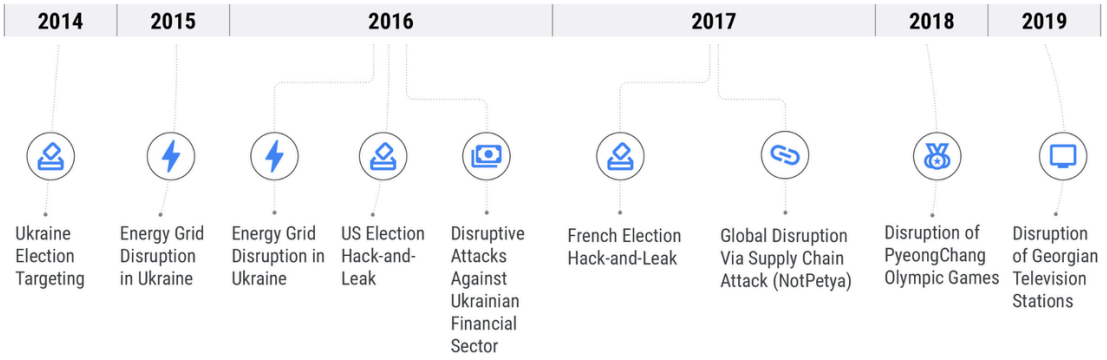

Figure 3: Timeline of consequential pre-war APT44 operations

Due to its history of aggressive use of network attack capabilities across political and military contexts, APT44 presents a persistent, high severity threat to governments and critical infrastructure operators globally where Russian national interests intersect. The combination of APT44's high capability, risk tolerance, and far-reaching mandate to support Russia's foreign policy interests places governments, civil society, and critical infrastructure operators around the world at risk of falling into the group's sights on short notice.

We also judge APT44 to present a significant proliferation risk for new cyber attack concepts and methods. Continued advancements and in-the-wild use of the group's disruptive and destructive capabilities has likely lowered the barrier of entry for other state and non-state actors to replicate and develop their own cyber attack programs. Russia itself is almost certainly alert to and concerned about this proliferation risk, as Mandiant has observed Russian cybersecurity entities exercise their ability to defend against categories of disruptive cyber capabilities originally used by APT44 against Ukraine.

Looking Ahead

APT44 will almost certainly continue to present one of the widest and highest severity cyber threats globally. It has been at the forefront of the threat landscape for over a decade and is responsible for a long list of firsts that have set precedents for future cyber attack activity. Patterns of historical activity, such as efforts to influence elections or retaliate against international sporting bodies, suggest there is no limit to the nationalist impulses that may fuel the group's operations in the future.

As Russia's war continues, we anticipate Ukraine will remain the principal focus of APT44 operations. However, as history indicates, the group's readiness to conduct cyber operations in furtherance of the Kremlin's wider strategic objectives globally is ingrained in its mandate. We therefore assess that changing Western political dynamics, upcoming elections, and emerging issues in Russia's near abroad will also continue to shape APT44's operations for the foreseeable future.

Protecting the Community

As part of our research, we take various steps to protect customers and the community:

- Google's Threat Analysis Group (TAG) uses the results of our research to improve the safety and security of Google's products.
    - Upon discovery, all identified websites and domains are added to Safe Browsing to protect users from further exploitation.
    - All targeted Gmail and Workspace users are sent government-backed attacker alerts, notifying them of the activity, encouraging potential targets to enable Enhanced Safe Browsing for Chrome, and ensuring them that all devices are updated.
- Where possible, Mandiant sends victim notifications via the Victim Notification Program.
- If you are a Google Chronicle Enterprise+ customer, Chronicle rules were released to your Emerging Threats rule pack, and IOCs are available for prioritization with Applied Threat Intelligence.
- A VirusTotal Collection featuring APT44-related indicators of compromise is now available for registered users.

We are committed to sharing our findings with the security community to raise awareness, and with companies and individuals that might have been targeted by these activities.

Read the APT44 report for our full analysis of this group, a detailed list of malware used by APT44 since 2018, hunting rules for detecting the malware, and a list of Mandiant Security Validation actions organizations can use to validate their security controls.

Posted in

- Threat Intelligence
