# TYPICAL TACTICS AND SCENARIOS OF ACTIVITY OF GRU RF APT GROUPS

This report examines a typical scenario of cyber threats posed by APT groups within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU GS AF RF); however, for convenience, the report will also use the former name — Main Intelligence Directorate (GRU). This report is based on our previous reports on APT44 and APT28 and is supplemented with additional materials about them identified during the analysis. The structure of the GU GS AF RF has also been analyzed.

In the context of this report, the term “APT” serves as an analytical label which, when combined with a specific APT group number, is attributed to a particular unit of the GU GS AF RF. These attributions are based on open sources. We do not assert the existence of a “single concept,” but rather model possible patterns; therefore, a “hypothetical model” in the context of this report represents an assumption about how military units distribute functions within a unified ecosystem. The term “APT” is merely an analytical abstraction, whereas the actual operational units are specific military units with their own infrastructure, symbolism, and hierarchy. From the perspective of Russian legislation, these structures have the status of a legitimate instrument of state policy operating within the military command system. The purpose of this study is to systematize known tactics, techniques, and procedures used by Russian APT groups within the GU GS AF RF. Particular attention in the report is given to identifying correlations between different groups and their activities, which helps to build a comprehensive picture of the organizational and operational structure of the GRU.

Organizations perceive APT groups through the lens of their own data and classification systems. The first references to incidents related to APT groups date back to approximately the 2000s, when computer incident response teams in the United States and the United Kingdom published alerts describing targeted, socially engineered emails containing trojans designed to steal sensitive information. Organizations have been studying APT groups for over 20 years, so today’s findings and conclusions are the result of long and meticulous work.

The data presented in this report are based on open sources published from 2014 to the present. The dynamic nature of intelligence data, changes in adversary tactics, and the continuous updating of knowledge bases such as MITRE ATT&CK (which relies on public reports) necessitate treating the listed TTPs as current at the time of writing, with the understanding that they may evolve in the future.

# ORGANIZATIONAL MODEL OF INFORMATION OPERATIONS UNITS OF THE GU GS AF RF

After the collapse of the Soviet Union, information operations units were integrated into newly formed structures within the Main Intelligence Directorate of the Russian Federation in November 1991, forming the basis for the future Information Operations Troops of the GU GS AF RF, as noted in the 2026 CheckFirst report, which analyzed the military information operations units of the GU GS. In their report, they suggest that these units are integrated into a special directorate that consolidates three main areas of competence under a single command: psychological operations, encryption and cryptoanalysis, and computer network operations.[1]

The Main Directorate of the General Staff of the Armed Forces of the Russian Federation is the central body for military intelligence management. Within this system, the Information Operations Troops (IOT) occupy a special place, serving as a tool for implementing the strategy of “information confrontation,” where cyberattacks and propaganda are considered as a unified whole. In Russian military doctrine, technical measures within the concept of “information confrontation” also include computer network operations. In this model, the system of information operations troops defines the direction of activity, while the military unit performs defined functions, where an “APT group” serves as an analytical representation of observed activity, that is, a stable behavioral profile of a unit’s activity in cyberspace.


Fig. 1.1 – Structure of the “Information Operations Troops” of the GRU RF. ©CheckFirst 2026

| MILITARY UNIT | SUBUNIT | LOCATION | AREA OF ACTIVITY |
|---|---|---|---|
| INFORMATION-PSYCHOLOGICAL OPERATIONS | | | |
| 54777 | 72nd Special Service Center | Senezh | Main Center for Management of Information Operations |
| 03126 | 2148th Unit | Sertolovo-2 | Europe, NATO, Baltic States |
| 03127 | 2156th Unit | Tver | Unknown |
| 03128 | 2140th Unit | Bataysk | Ukraine, Caucasus |
| 03132 | 2047th Unit | Chita | Asia |
| 03134 | 2040th Unit | Khabarovsk | East Asia |
| 03138 | 2059th Unit | Yekaterinburg | Central Asia |
| 20697 | | Saint Petersburg | Ukraine, Baltic States |
| DECRYPTION AND CRYPTOANALYSIS | | | |
| 20766 | | Khabarovsk | |
| 26165 (APT28) | | Moscow | Europe, America |
| 48707 | | Kursk | |
| 78430 | | Yekaterinburg | |
| COMPUTER NETWORK OPERATIONS | | | |
| 20978 | | Moscow | |
| 74455 (APT44) | | Khimki | Europe, America |

Table 1.1 – Structure reconstructed based on open sources (may differ from actual) [2][3][4][5][6][7]

It should be noted that in the CheckFirst investigation, Unit 20697 is included within the department of decryption and cryptoanalysis; however, the OSINT investigation by “Toronto Television” describes the activities of Unit 20697 as being responsible for conducting information-psychological operations.[8] This is supported by the activities of its personnel, who specialize in political science, communications, psychology, and related fields.

According to open-source data, there are also several units subordinate to Unit 55111 that serve as centers in each military district:

- Unit 76836 (706th Information Confrontation Center, Western Military District);
- Unit 76853 (711th Information Confrontation Center, Southern Military District);
- Unit 76854 (Information Confrontation Center, Central Military District);
- Unit 76862 (738th Information Confrontation Center, Eastern Military District).

The central governing body is the 72nd Special Service Center in Senezh, which oversees regional PSYOP units with a geographically distributed scope of responsibility (Europe, NATO, Ukraine, the Caucasus, Asia, etc.). The information-psychological operations units of the GU GS likely perform the function of transforming data obtained by other units into psychological influence, coordinating information campaigns against specific targets. As noted by CheckFirst in its report: “Taken together, these findings suggest that the psychological operations unit manages a significant and structured apparatus designed to conduct psychological operations not only against foreign target audiences, but also against the Russian domestic audience.”

Decryption and cryptoanalysis constitute the second key component within the Information Operations Troops system. As stated in the CheckFirst report, the analysis of award insignia made it possible to identify these units as a distinct direction within the GU GS structure. Formally, these units are responsible for communications security, but in practice they form the foundation of Russia’s cyber operations. This is explained by the post-Soviet transformation, where instead of intercepting radio signals, they began intercepting digital communications, which requires not only decryption but also system intrusion to gain access to encrypted data.

Based on public reports, the modern role of computer network operations units is revealed through functions such as cyber sabotage, intelligence collection through the compromise of network devices, and information operations via proxy structures or controlled assets.

Hypothetically, several activity models can be proposed to outline the roles performed by all units in interaction with APT groups; however, this requires further study of other units as separate components of the overall ecosystem. Therefore, the question of the specific roles performed by other military units within this structure remains open for further research.

# Personnel Indicators of Institutionalization of Cyber Units

Particular attention should be paid to personnel changes within the system of state governance of the Russian Federation. A notable example is the resignation of Pavel Mykhailovych Konovalchyk from the position of Assistant to the Secretary of the Security Council of the Russian Federation (assistant to Sergey Shoigu), which he had held since July 2024. “Pavel Mykhailovych Konovalchyk is a highly qualified strategic-level manager; he is being transferred in a planned manner to another position with a promotion in the field of information-analytical support of national security.”

Pavlo Konovalchyk is a military intelligence officer with a technical background. According to a CNA investigation, he was linked to Unit 26165 and headed the Information Operations Troops.

Based on the statement of the Security Council of the Russian Federation, it can be assumed that his professional activities will be related to intelligence and information operations. His transfer to a higher position may indicate an increasing role of the information-analytical and cyber component in the system of strategic planning of national security of the Russian Federation. In our view, this may indicate further institutionalization of information and cyber operations within the state security system of the Russian Federation, where technical units operate within a broader system of strategic planning coordinated at the level of the Security Council or other interagency structures. A similar case was observed in 2021, when GRU officer Oleksandr Starunskyi, associated with psychological operations units, assumed the position of scientific advisor to the same Security Council.[9] The recurrence of such appointments allows them to be viewed as a pattern of deliberate promotion of technical and operational cyber personnel into the higher echelon of strategic planning.

It is likely that the integration of specialized personnel at the level of the Security Council indicates a gradual shift in the functional status of cyber and information operations within the state governance system of the Russian Federation — from a tool for implementing strategic decisions to a component involved in their formulation. If this trend is sustained, it will have implications not only for the operational activity of GU GS units, but also for the logic within which these operations are planned and executed.

# INTELLIGENCE-ORIENTED UNIT 26165 (APT28)

We previously noted that the activity of this unit was observed in 2004; however, its origins date back to the Cold War period, when it functioned as a communications unit operating in the fields of military intelligence and encryption. The unit was known as both the “Decryption Service” and the “85th Main Special Service Center 33.” Historically, Unit 26165 was engaged in decrypting intercepted tactical military communications within the USSR and abroad. For this purpose, the unit used the “Bulat” system, developed in the 1970s by the Kvant research center for the needs of the 16th Directorate of the KGB — the predecessor of the 16th Center of the FSB. Kvant continues to be accused of developing technologies for the benefit of technical units of Russian intelligence services.


Fig. 1.2 – Insignia of Unit 26165. ©CheckFirst 2026

The activities of APT28 have always been driven by Russia’s geopolitical interests. In the 2000s, attacks were observed in the Caucasus region, where, amid instability, Russia sought to maintain its geopolitical influence. Georgia held particular significance, as under President Saakashvili it pursued closer ties with the West and NATO membership. This was perceived by the Kremlin as a threat to its interests, culminating in the Russo-Georgian War in August 2008.

Since 2011, APT28 has been sending emails to journalists and individuals associated with government institutions containing information of interest to the recipient, while simultaneously registering websites that mimic legitimate news outlets. Today, this trend has not only persisted but has become widespread, with APT28 operating globally and targeting multiple countries simultaneously.

Whereas previously the focus was primarily on post-Soviet states, the geography of attacks now spans all of Europe, North America, and the Middle East. Ukraine remains a key priority, with central government bodies consistently targeted by hackers. This is evidenced by a recent attack (January 2026) exploiting a Microsoft Office vulnerability (CVE-2026-21509), which researchers from Zscaler ThreatLabz attributed to APT28 due to a significant overlap in tools, techniques, and procedures (TTPs). Users in Central and Eastern Europe were targeted, including Ukraine, Slovakia, and Romania, where social engineering lures were crafted in both English and localized languages to target users in those respective countries.[10][11][12]


Fig. 1.3 – Pennant “IO Troops of the GU GS” – military information operations. The symbolism of Unit 26165 is highlighted in red.

The unit consists of several teams focused on different aspects of GRU cyber and hybrid operations. The three main teams include the operational group (Ops), the operations development group (DevOps), and the operational infrastructure group. As of December 2025, Boris Antonov holds a senior leadership position within Unit 26165, where he leads the activities of the operational team. He was first exposed by the FBI and the U.S. Department of Justice in 2018. Aleksey Lukashev, Ivan Yermakov, and Andrey Baranov were members of this team.

Sergey Morgachov was responsible for leading the developers within the unit. This team is responsible for the development and management of Unit 26165's malware, including X-Agent and the data exfiltration tool known as X-Tunnel. Mykola Kozachok, Artem Malyshev, and Pavlo Yershov were members of this team.

Anatoliy Istomin was responsible for leading the operational infrastructure group. His subordinates included Ihor Bochka, Oleksiy Umets, Sergey Vasyuk, and others. This group and its members carry out a range of operational activities, including procurement of infrastructure, testing and configuration, data exfiltration, open-source research, and intelligence support for the unit's operations focused on Ukraine.

Although Unit 26165 primarily focuses on cyberattacks, it may also operate in the physical domain. In 2018, the Dutch government stated that in April, four GRU agents were detained in The Hague while attempting to hack the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW). The OPCW was investigating the chemical attack in Syria and the nerve agent attack on Sergey Skripal, a former Russian spy in the United Kingdom. According to the Dutch authorities, one of the four agents had previously been in Malaysia, where he was involved in the investigation of the aviation disaster involving "Boeing 777, MH17," shot down over eastern Ukraine in 2014, one of the deadliest air disasters in history.

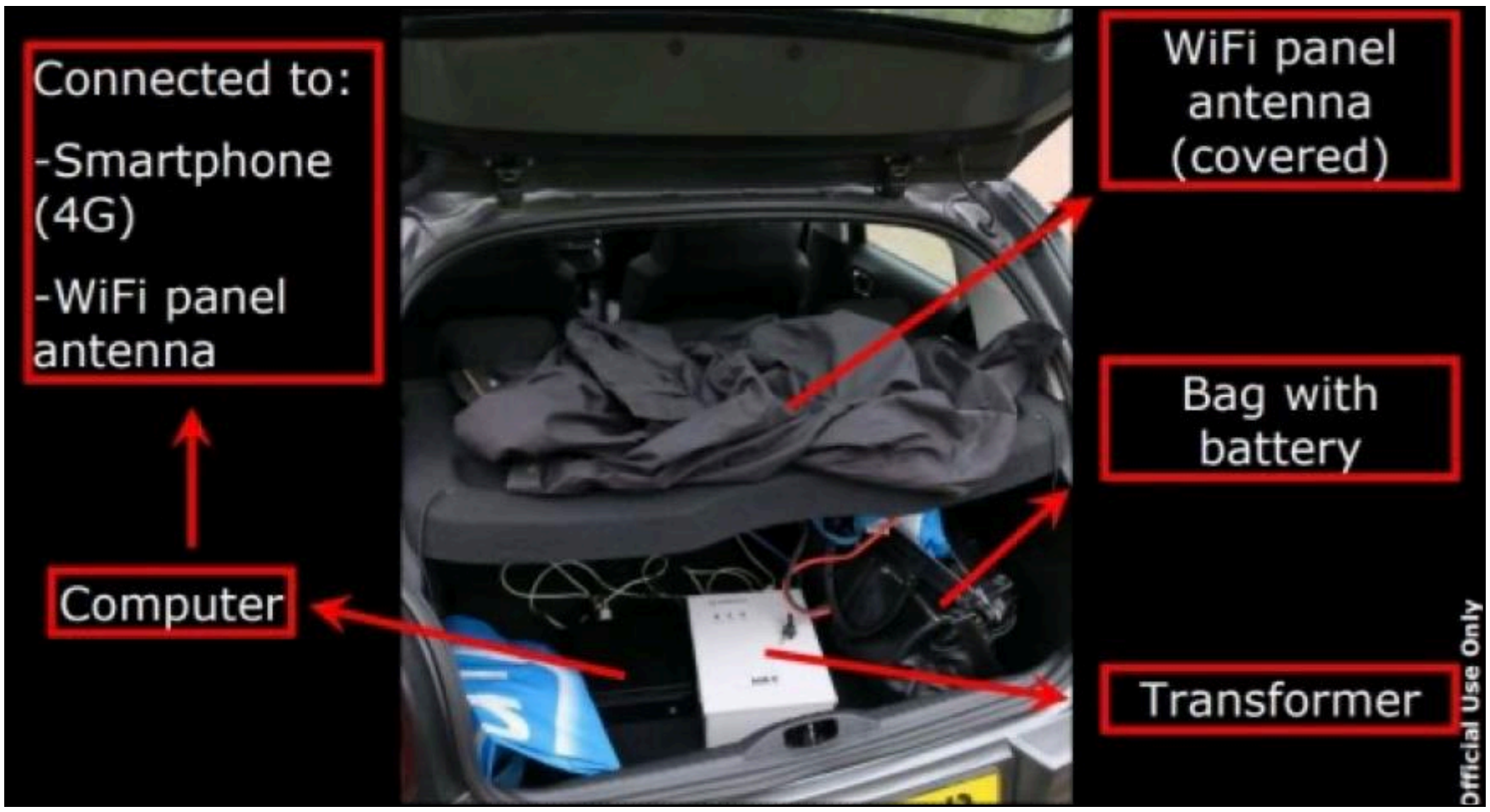


Fig. 1.4 – Equipment used by Unit 26165 personnel in the attack against the Organisation for the Prohibition of Chemical Weapons in The Hague (2018).

The UK government portal highlights the role of Unit 26165 in conducting online reconnaissance of civilian shelters in Mariupol and Kharkiv on March 15, 2022.

On March 16, 2022, the Armed Forces of the Russian Federation deliberately carried out artillery strikes on the Mariupol Drama Theatre, resulting in the deaths of civilians and children who were sheltering there. [14]

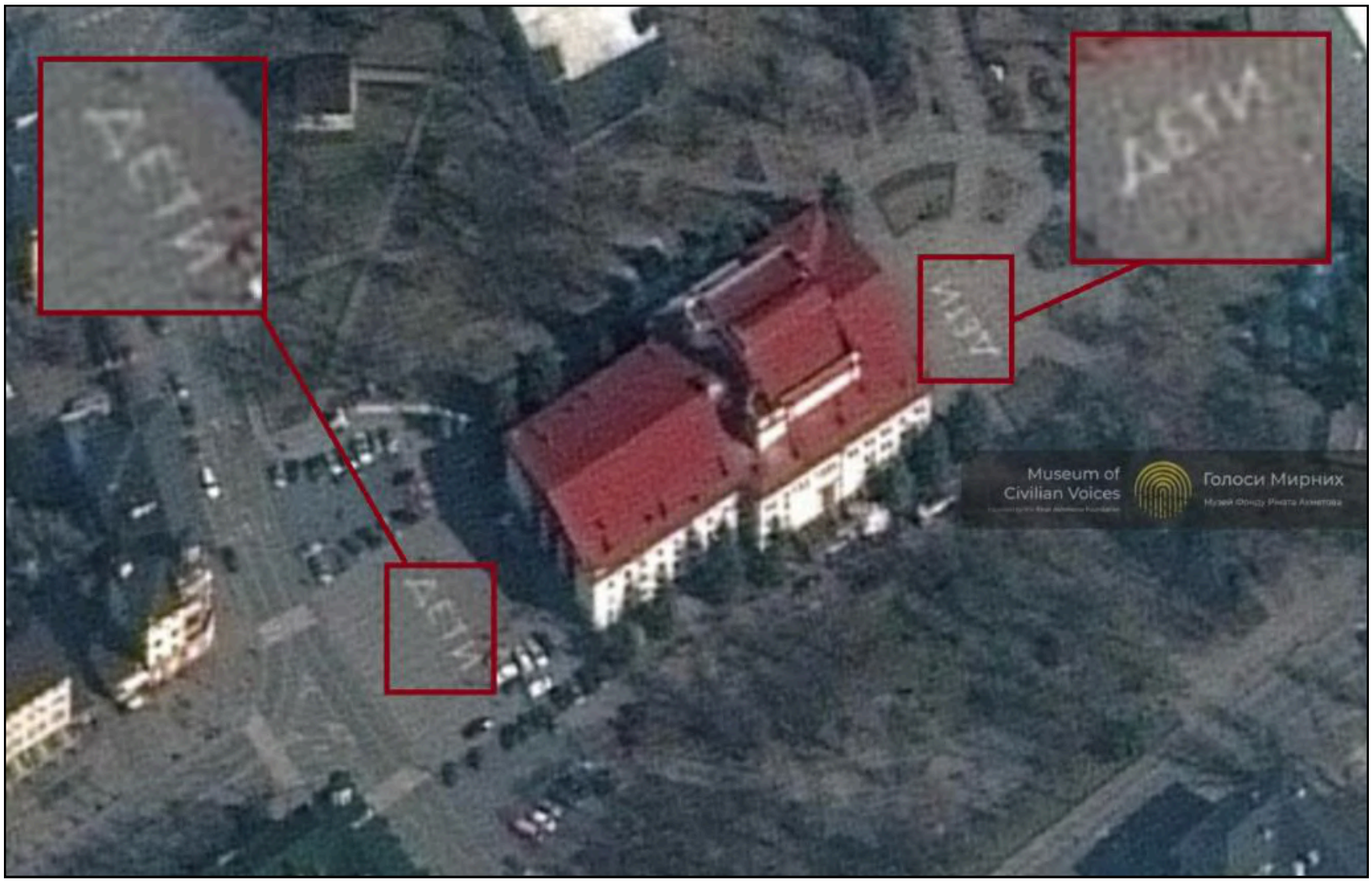


Fig. 1.5 – The inscription “CHILDREN” near the drama theatre in Mariupol.

Due to the fact that the Russian armed forces failed to achieve their military objectives, while Western countries increased support for Ukraine’s defense, Unit 26165 expanded its targeting to logistics structures and technology companies involved in the delivery of foreign aid. This campaign lasted for more than two years and was documented in a joint advisory by CISA/NSA/FBI and partner agencies from eleven countries dated May 21, 2025.

Unit 26165 targeted a wide range of logistics and technology providers, compromising organizations across virtually all modes of transportation—air, maritime, and rail—in NATO countries, Ukraine, and international organizations. A separate intelligence vector involved the use of video surveillance cameras.

Starting from March 2022, Unit 26165 conducted large-scale campaigns to compromise IP cameras. More than 80% of the compromised cameras were located in Ukraine, with moderate concentrations in Romania and Poland. As a result, civilian video surveillance infrastructure—municipal traffic cameras, monitoring systems of ports, railway stations, and border crossings—was transformed into a tool of strategic intelligence.

For the analysis of technical methods and specifics of APT28's use of techniques, we referred to MITRE ATT&CK. The actual number of attacks and identifiers is significantly greater than those mentioned in Appendix A on the technical characteristics of APT groups. Typically, techniques are used in a logical sequence that depends on the objective and tactics of the attack. Additionally, the quantitative dominance (frequency of mentions) of certain tactics in open sources may result from better detection of specific tools rather than an objective assessment of their usage.

The analysis of the software used showed that APT28 utilizes a combination of proprietary-developed software, open-source tools, and system utilities or tools (Living off the Land – LotL) embedded in operating systems (Windows, Linux). Some software names were assigned by researchers and may not correspond to the original names of the tools.

An interesting observation is that a significant portion of the software is developed directly by APT28 operators or affiliated developers. APT28 maintains its own malware families, such as "Zebrocy," which is responsible for initial access; "Sofacy," responsible for primary backdoors and espionage; and "X-Agent," used for mobile and cross-platform espionage. In addition, APT28 combines custom software with open-source tools and LotL utilities. It is worth noting that most indicators of compromise (IoCs) have a limited lifespan, as APT28 regularly changes its infrastructure, domains, and files while maintaining consistent behavioral patterns.

The cyber threat detection and response team at Sekoia analyzed infected files used in one of APT28's attacks, which were delivered to Ukrainian military personnel via the Signal messenger. Sekoia notes that the prevalence of documentation related to wounded individuals may also indicate a potential interest in injured servicemen, their command structures, and their units, which could be used to assess attrition, operational readiness, or psychological resilience within specific units.

A similar pattern is observed with logistics-related lure documents, which are used to establish legitimacy among military administrative personnel in order to collect intelligence on combatants at the front line. [13]

## UNIT OF DESTRUCTIVE OPERATIONS IN CYBERSPACE 74455 (APT44)

The activity of Unit 74455 can be traced back to the 2000s, although the group became publicly known in 2009. On September 3, 2014, iSIGHT Partners identified a phishing campaign that exploited the zero-day vulnerability CVE-2014-4114. This attack coincided with the NATO summit on Ukraine in Wales and became the first documented operation of APT44.

In the report dated January 19, 2026, we described the group's activities, where APT44 represents a classic example of a "domain-oriented" unit, whose existence is defined by its area of competence: destructive operations and cyber sabotage. Unlike APT28 (espionage), APT44 focuses on destructive attacks, where the objective is often the destruction of information or damage to systems.

One of the key characteristics and an important “signature” of APT44 is the creation and management of proxy structures that present themselves as “grassroots hacktivists.” A Mandiant (2022) study found that moderators of the Telegram channels “XakNet Team,” “Infoccentr,” and “CyberArmyofRussia_Reborn” coordinate their operations with APT44. The Insider also described a case where the “CyberArmyofRussia” channel published information about a successful attack half an hour before it actually occurred.

The “Solntsepek” channel, initially created to publish personal data of Ukrainian servicemen, according to Mandiant, after rebranding in 2023, also became a channel through which the GRU “leaks” data obtained during its intrusions. [15][16]


Fig. 1.6 – Commemorative insignia marking 10 years of Unit 74455

Unit 74455, which forms the core of the GRU’s psychological warfare component, closely cooperates with “technical” units and has been conducting cyberattacks against organizations since at least 2014. This unit is attributed with the creation and dissemination of malware used for spoofing during the 2016 U.S. presidential elections, the NotPetya malware, and attacks on Ukraine’s energy infrastructure. [17]

Russian intelligence services compete with each other and often conduct similar operations against the same targets. Therefore, it is sometimes difficult to make precise attribution assessments. However, within the GRU, attacks may also be carried out jointly; for example, according to the Mueller indictment, Unit 74455 used, in Russia’s interests, information stolen by Unit 26165.

In June 2016, in the midst of the U.S. presidential election campaign, a WordPress blog was created under the name Guccifer 2.0. Posing as a lone Romanian hacker, he published his first post containing stolen DNC (Democratic National Committee) documents. Almost simultaneously, the online platform DCLeaks, which presented itself as an initiative of American “hacktivists,” began publishing personal correspondence of high-ranking U.S. officials and military personnel. Subsequently, 300 emails from Republicans and personal phone numbers of more than 200 legislators were released. On August 15, 2016, files from the George Soros Foundation were published, containing internal work plans and information about the foundation’s activities worldwide.

In August 2016, a congressional candidate from Florida contacted Guccifer 2.0 requesting information about his opponent. Guccifer 2.0 provided the requested stolen data. Republican strategist Aaron Nevins also contacted Guccifer 2.0. He created a Dropbox account, to which Guccifer 2.0 uploaded 2.5 gigabytes of data. Nevins analyzed the data, published the results on his blog, and sent the link to Guccifer 2.0, who then forwarded it to Trump adviser Roger Stone. The 2018 indictment by the U.S. Department of Justice states that:

- Guccifer 2.0 and DCLeaks were controlled by GRU officers;
- Unit 26165 conducted the intrusion;
- Unit 74455 was involved in dissemination and the information component.

Infrastructure and social media accounts administered by the department of Aleksey Potyomkin (an officer of Unit 74455) were used to facilitate the publication of stolen documents via DCLeaks and Guccifer 2.0. Servicemen of Unit 74455 rented a server in Malaysia to host the website, managed it, and created a false image of “American hacktivists.” They set up a WordPress blog, ran the Twitter account Guccifer_2, and communicated with journalists from Vice and The Hill. According to the investigation, the objective of the operation was to influence the presidential election and discredit the Democratic Party.

According to Mandiant, the attack on an energy facility in October 2022, attributed to “Sandworm”—a GRU Unit 74455 subgroup—is a rare example of a cyber incident that disrupted the physical operation of the targeted facility. According to researchers, the intrusion also involved a previously unknown technique for disrupting industrial control systems and operational technology. This was not only the first publicly known power outage caused by a cyberattack since the beginning of the war, but also the first case where such an incident coincided with a missile strike.

In turn, researchers from the Economic Security Council of Ukraine and the independent communications agency “Truman” stated that Russia coordinated this activity with psychological operations to confuse its targets. The researchers noted that Russia carried out a series of cyberattacks on energy infrastructure at the end of 2022 before launching massive missile strikes. At the same time, Moscow initiated a propaganda campaign aimed at shifting responsibility for the power outages caused by these attacks onto the Ukrainian government, state authorities, and private energy companies. [18][19]

The campaign involving “Infamous Chisel” was attributed to APT44 in a joint technical report by Five Eyes agencies (NCSC, CISA, NSA, FBI, ASD, CCCS, NCSC-NZ) dated August 31, 2023, which provided a detailed analysis of malware deployed against Android devices used by Ukrainian military personnel. In parallel, the Security Service of Ukraine (SBU) published its own report attributing the campaign to “Russian military intelligence and its hackers.” According to Illia Vitiuk, Head of the SBU Cybersecurity Department, responsibility for the cyberattacks lies directly with the GRU-controlled group Sandworm (APT44).

A critically important finding by the SBU concerns the initial infection vector. According to the agency’s cyber experts, the adversary captured Ukrainian tablets on the battlefield in order to spread malware and exploit existing access to infiltrate military networks. Thus, the physical capture of a device during combat became a vector for subsequent cyber intrusion—constituting a documented example of the integration of kinetic and cyber methods at the tactical level. The SBU also noted that оперативне реагування allowed them to block attempts to gain access to sensitive information regarding the activities of the Armed Forces of Ukraine, the deployment of defense forces, and their technical support. [20]

## OPERATIONAL-TARGETED UNIT 29155 (CADET BLIZZARD)

Unit 29155 is a hybrid military unit that focuses on both physical and cyber sabotage. This unit differs from APT28 and APT44 in its purpose and is not part of the Information Operations Forces system; however, to demonstrate its impact on cyberspace, we include this case, as Microsoft identifies its cyber component as a “threat group.” Additionally, the UK government portal lists sanctions imposed on Unit 29155 (Cadet Blizzard) alongside Units 26165 and 74455. The unit, composed largely of young recruits operating under experienced leadership, possesses a range of capabilities but is characterized by poor discipline and a chaotic approach to conducting operations. [14][21][22]

Cadet Blizzard is the cyber component of Unit 29155, as confirmed by assessments from CISA and the FBI. Unlike APT groups, Unit 29155 is a “task-oriented” unit that operates across multiple domains, where cyber components may be integrated as needed. Its activity can be described as project-based, where the application of resources depends on the operational objective. Examples include the poisoning of the Skripals in Salisbury, the explosions in Vrbětice, and, in January 2022—one month before the full-scale invasion—Cadet Blizzard deployed the WhisperGate wiper against IT systems of Ukrainian government institutions. Microsoft also notes that “...at least one Russian private sector organization provided material support to Cadet Blizzard during the destructive WhisperGate attack.” According to Microsoft’s assessment, Cadet Blizzard has been active since at least 2020, with initial compromises targeting Eastern European government and technology sectors beginning in April 2021. [23]

“In August 2021, five months before Russia’s full-scale invasion, hackers from Unit 29155 attempted to escalate tensions between Ukrainian nationalist units and the administration of Volodymyr Zelensky… …Following a typical false-flag operational pattern, Stigal recruited dozens of low-level informants to pose as members of the Azov Regiment—one of Ukraine’s most capable paramilitary formations, which had drawn attention in the West due to the right-wing views of some of its members.

He went further and established contact with at least two senior Azov commanders, posing as a leader of the Chechen dissident organization Ichkeria, which opposes Chechen leader Ramzan Kadyrov, and offered them an alliance against Zelensky. Misled by Stigal, at least one Azov commander agreed to the offer of assistance.” The Insider did not disclose the identity of the interlocutor, who is currently serving in the Armed Forces of Ukraine, as he was unaware that he was cooperating with Russian intelligence (Stigal was acting on behalf of the pro-Ukrainian head of the Chechen Republic of Ichkeria in exile, Akhmed Zakayev).

Stigal recruited dozens of “low-tier” agents who were supposed to pose as members of the Azov Battalion and carry out provocations. Among the files found on the hackers’ server was a folder titled “Graffiti in Cities,” which contained images of offensive messages directed at Zelensky, painted by provocateurs on the walls of Ukrainian cities (for which they were paid between one and five dollars). A GRU-recruited Bulgarian journalist, Dilyana Gaytandzhieva, was also involved in this operation. In 2022, she published and later deleted a piece describing a supposed “conflict” between Azov and the GRU, framed in a way that suggested Azov fighters were allegedly receiving money from Kadyrov’s forces. [24]


Fig. 1.7 – Example of graffiti funded by the GRU of the Russian Federation. ©The Insider

As noted by Paul Chichester, Director of Operations at the NCSC: “The exposure of Unit 29155 as a capable cyber actor illustrates the importance that Russian military intelligence places on the use of cyberspace to conduct its unlawful war in Ukraine and pursue other state priorities.”

# TACTICS OF APT GROUP EMPLOYMENT

This playbook is an analytical reconstruction of the operational logic of APT groups within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU GS), operating in cyberspace. Its purpose is to explain how strategic objectives of the military-political leadership are transformed into concrete actions of military units attributed with an APT profile.

The initiation of cyber operations by GU GS units is not random and is linked to specific events. Strategic triggers include political or military developments that create an increased demand for intelligence or information-psychological influence, such as international political crises, military conflicts, election campaigns in foreign states, diplomatic disputes, the imposition of international sanctions, resource crises, military breakthroughs, protests or political instability within a state, interethnic or interreligious conflicts, international scandals, and similar events. Under such conditions, cyber operations may be used for intelligence gathering, influencing the information space, or exerting additional pressure on target states.

Operational triggers are usually associated with specific opportunities or conditions that enable or simplify the execution of an attack. In such cases, the decision to conduct an operation may be based on the availability of favorable technical conditions. Additionally, certain operations may be initiated based on opportunistic access. In these scenarios, operations may have an experimental or reconnaissance nature and be used to further develop access (e.g., access to compromised servers or networks, credential leaks, etc.).

Analysis of the operational activity of these APT groups demonstrates that the tactics employed are not a fixed set. They vary depending on the type of target organization and are influenced by multiple factors, not solely by the intent to use a particular tool. A purely signature-based approach often hinders effective countermeasures and necessitates context-driven threat modeling.

Let us consider a generalized playbook model:

1. **Strategic objective.**
The deployment of the GU GS units (APT groups) analyzed in this report begins with the formulation of a strategic objective at the level of military-political leadership or relevant military intelligence structures (e.g., Information Operations Forces). This stage involves defining the overall purpose of the operation, which may include intelligence collection, sabotage, acquisition of compromising material, destabilization of infrastructure, etc.

2. **Target identification.**
At this stage, the process of specifying targets is carried out, where strategic objectives within the “cyber units department” are transformed into a list of specific institutions, networks, or infrastructure objects that may contain the required information or hold critical importance for political influence, state functioning, institutional operations, or specific sectors. This process is iterative, as information obtained at later stages may lead to the redefinition or expansion of the initial list of targets.

3. **Reconnaissance.**

At the reconnaissance stage, systematic collection of information about selected targets and their infrastructure is conducted. A significant portion of this activity is based on the use of open sources. Technical reconnaissance is also performed, including analysis of domain infrastructure, mail servers, network services, and other elements of IT and OT environments. The objective of this stage is to identify potential entry points into information systems, conduct supply chain analysis—examining contractors and partners of the organization as potential attack vectors—and establish personal connections of individuals, which may also serve as potential attack vectors.

4. **Preparation stage.**

This stage involves the creation of technical means that will be used to penetrate the target system. It typically includes the registration of domains that mimic legitimate resources, preparation of phishing pages, configuration of servers, or modification of malware. Infrastructure is often built using proxy servers, compromised websites, or legitimate cloud services to complicate detection and blocking.

At the same time, documents or messages used for social engineering may be prepared.

5. **Initial access.**

Initial access to the system is achieved through the use of social engineering methods or technical vulnerabilities. Targeted phishing is commonly employed, aimed at specific individuals who have access to internal organizational services or are designated targets. Vulnerabilities in network services or corporate access systems may also be exploited.

6. **Persistence.**

After gaining access to the system, attackers attempt to ensure long-term access to the compromised environment. Various persistence mechanisms may be used to restore access after operating system reinstallation or partial remediation of the attack’s effects, such as the use of bootkits at the OS kernel level, UEFI rootkits, etc. Control over the access channel is critically important for subsequent stages of the operation, as it enables gradual expansion of control within the network.

An important transformation in modern cyber operations is the shift from one-time attacks to long-term strategic persistence within adversary networks. In earlier models, the primary objective was to accomplish a specific task, after which access might be lost or intentionally not maintained. Today, access to an information system is increasingly viewed as a long-term strategic asset that can be leveraged over extended periods. This model is evident in the activities of Unit 26165, which in many cases performs the role of establishing access and conducting long-term intelligence collection. The acquired access may be retained over time and later utilized by other units, particularly 74455, to execute destructive or information operations.

7. **Credential access.**

After establishing persistence within the system, attackers seek to obtain user and administrator credentials, as this significantly expands their capabilities within the network and enables access to a broader range of information. Using specific tools and techniques, they may capture passwords, obtain authentication tokens, or leverage existing accounts for further actions.

8. **Lateral movement.**

The use of legitimate protocols and the availability of administrative privileges allow attackers to move within the organization’s network, compromising additional systems and servers. In this way, they expand their area of control and gain access to more protected network segments where more sensitive information may be stored.

9. **Internal reconnaissance.**

In parallel with lateral movement, internal reconnaissance is conducted. Its purpose is to identify key information assets, servers, and management systems. Particular attention is paid to file storage systems, email systems, databases, and other components that may contain valuable information. In the case of attacks on infrastructure, industrial control systems and technological networks are additionally analyzed.

10. **Data collection.**

After identifying the required resources, the data collection phase begins. Depending on the nature of the operation (intelligence or destructive), its primary objectives are defined. Although such operations focus on different technical aspects, there is often overlap between them. During a destructive attack, access to valuable information may also serve as a strategic component at the level of a specific operation or campaign.

11. **Command & Control.**

To coordinate further actions, a communication channel is established between the compromised system and the operators’ infrastructure. Through this channel, commands, malware updates, and execution results are transmitted. The use of encrypted or obfuscated traffic helps conceal this communication within legitimate network activity.

12. **Exfiltration**

The transfer of data outside the target network may occur through various methods designed to evade detection by monitoring systems. Data exfiltration can be performed gradually, in small volumes, to disguise the activity as normal network traffic.

13. **Support the organization’s activities: https://donate.shum-ng.org/**

The final stage, in most cases—but not always—depends on the initial objective of the operation. Typically, the outcome involves the acquisition of information used for further analysis or influence, disruption of system operations, destruction of data, or disabling elements of infrastructure.

14. **Information operations.**

In some cases, the results of a cyber operation are used in information campaigns. The obtained materials may be published in open sources or disseminated through intermediary platforms to create an information-psychological effect. In this way, a cyber operation becomes part of broader information-psychological activity aimed at shaping a narrative or interpretation favorable to the initiator of the operation. An example of this includes APT44-controlled proxy channels mentioned in the section on Unit 74455.

The reconstructed playbook demonstrates that cyber operations are not conducted in isolation by individual APT groups, but rather constitute part of a broader operational process in which different units perform defined functions at various stages of the operation. Within this model, Unit 26165 focuses on long-term intelligence collection, access preparation, and the development of technical capabilities for subsequent actions. Unit 74455 specializes in delivering cyber effects, including destructive operations and attacks on critical infrastructure.

According to the reconstructed playbook, a typical operational cycle includes sequential stages beginning with a strategic objective and, in some cases, followed by information or psychological exploitation of the attack results. At the same time, the analysis indicates that this operational cycle is not always fully implemented. In many cases, units act autonomously, executing only specific stages. This suggests that the cyber operations system of the GU GS of the Armed Forces of the Russian Federation combines centralized strategic planning with relative tactical autonomy of executing units.

This playbook indicates the existence of a structured model for conducting cyber operations, in which intelligence, destructive, and hybrid components can be combined to achieve various effects across cyber, informational, and political domains.

The analysis of GU GS unit activities demonstrates that modern cyber operations are increasingly integrated into a broader system of strategic competition between states. In this context, the activities of the analyzed APT groups are viewed as part of a long-term operational model aimed at establishing strategic advantages in the digital domain.

The reconstructed playbook reflects a relatively stable logic of action. A particularly important role in this model is played by the stage of long-term access persistence, which allows operators not only to collect information but also to build capacity for future influence operations.

An important trend is that network access is increasingly regarded as a strategic resource that can be leveraged over extended periods. This shifts the nature of cyber operations from one-off attacks to the establishment of persistent presence within an adversary’s digital infrastructure.

The analysis of documented operations reveals a recurring pattern in which cyberattacks in some cases preceded kinetic strikes and were coordinated with them in terms of timing and target audience. This trend alters the threat model for critical infrastructure operators, where a cyber incident under such conditions may not be an isolated event but rather an indicator of preparation for, or initiation of, kinetic impact against the same target. This suggests that the model of coordinated cyber-kinetic operations may potentially see broader strategic application.

# APPENDICES

## APPENDIX A. TECHNICAL CHARACTERISTICS OF APT GROUPS – MOST COMMON TECHNIQUES OF APT28

We compiled a list of the most characteristic techniques for APT groups using MITRE ATT&CK.

| ID | | NAME | USAGE |
|---|---|---|---|
| T1566 | .001 | Phishing: Spearphishing Attachment | APT28 sent spearphishing emails containing malicious Microsoft Office and RAR attachments.[37][10][11][3][22][17][21][16] |
| T1204 | .001 | User Execution: Malicious Link | APT28 has tricked unwitting recipients into clicking on malicious hyperlinks within emails crafted to resemble trustworthy senders.[14][16] |
| T1204 | .002 | User Execution: Malicious File | APT28 attempted to get users to click on Microsoft Office attachments containing malicious macro scripts.[37][17][16] |
| T1078 | | Valid Accounts | APT28 has used legitimate credentials to gain initial access, maintain access, and exfiltrate data from a victim network. The group has specifically used credentials stolen through a spearphishing email to login to the DCCC network. The group has also leveraged default manufacturer's passwords to gain initial access to corporate networks via IoT devices such as a VOIP phone, printer, and video decoder.[52][3][23][2] |
| T1078 | .004 | Cloud Accounts | APT28 has used compromised Office 365 service accounts with Global Administrator privileges to collect email from user inboxes.[2] |
| T1003 | | OS Credential Dumping | APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[47][3][14] |
| T1003 | .001 | LSASS Memory | APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[47][3] They have also dumped the LSASS process memory using the MiniDump function.[2] |
| T1003 | .002 | Security Account Manager | During APT28 Nearest Neighbor Campaign, APT28 used the following commands to dump SAM, SYSTEM, and SECURITY hives: reg save hklm\sam, reg save hklm\system, and reg save hklm\security.[27] |

| ID | | NAME | USAGE |
|---|---|---|---|
| T1003 | .003 | NTDS | APT28 has used the ntdsutil.exe utility to export the Active Directory database for credential access.[2]<br>During APT28 Nearest Neighbor Campaign, APT28 dumped NTDS.dit through creating volume shadow copies via vssadmin.[27] |
| T1210 | | Exploitation of Remote Services | APT28 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.[6][40][41] |
| T1114 | .002 | Email Collection: Remote Email Collection | APT28 has collected emails from victim Microsoft Exchange servers.[3][2] |
| T1567 | | Exfiltration Over Web Service | APT28 can exfiltrate data over Google Drive.[21]<br>During APT28 Nearest Neighbor Campaign, APT28 exfiltrated data over public-facing webservers – such as Google Drive.[27] |
| T1070 | .001 | Indicator Removal: Clear Windows Event Logs | APT28 has cleared event logs, including by using the commands wevtutil cl System and wevtutil cl Security.[5][3] |
| T1070 | .004 | Indicator Removal: File Deletion | APT28 has intentionally deleted computer files to cover their tracks, including with use of the program CCleaner.[3] |
| T1070 | .006 | Indicator Removal: Timestomp | APT28 has performed timestomping on victim files.[5] |

## SOFTWARE USED BY APT28

| ID | NAME | TYPE | DESCRIPTION |
|---|---|---|---|
| S0045 | ADVSTORESHELL | Custom | C2 backdoor with data archiving and keylogging |
| S0351 | Cannon | Custom | Email-based C2 backdoor. Screen capture and file discovery |
| S0023 | CHOPSTICK | Custom | Modular C2 framework. Keylogging and file search |
| S0137 | CORESHELL | Custom | C2 backdoor for persistence and local reconnaissance |
| S0243 | DealersChoice | Custom | Exploitation framework for browser/document exploitation and payload delivery |
| S0134 | Downdelph | Custom | Bootkit providing kernel-lvl persistence and stealthy DLL injection |

| | | | |
|---|---|---|---|
| S0502 | Drovorub | Custom | Linux malware toolkit with kernel rootkit and C2 agent |
| S0410 | Fysbis | Custom | Linux backdoor providing remote shell and persistence |
| S0135 | HIDEDRV | Custom | Stealth driver for file hiding and DLL injection |
| S0044 | JHUHUGIT | Custom | C2 implant using COM hijacking for persistence |
| S0162 | Komplex | Custom | macOS backdoor with C2 communication and hidden file exfiltration |
| S0397 | LoJax | Custom | UEFI rootkit providing firmware-lvl persistence |
| S0138 | OLDBAIT | Custom | Targeted credential harvesting |
| S0136 | USBStealer | Custom | Data exfiltration for air-gapped systems via USB. |
| S0314 | X-Agent (Android) | Custom | Android spyware with surveillance and data exfiltration |
| S0161 | XAgentOSX | Custom | macOS spyware with keylogging and screen capturing |
| S0117 | XTunnel | Custom | C2 tunneling tool providing traffic proxying and remote shell access |
| S0251 | Zebrocy | Custom | Multi-language initial access backdoor |
| S0250 | Koadic | Open Source | Post-exploitation framework with JScript/ VBScript RAT capabilities |
| S0002 | Mimikatz | Open Source | Credential dumping tool targeting LSASS and SAM |
| S1187 | reGeorg | Open Source | SOCKS proxy tool for internal network pivoting |
| S0174 | Responder | Open Source | LLMNR/NBT-NS poisoning for NTLM credential interception |
| S0183 | Tor | Open Source | Anonymization network used for C2 traffic concealment |
| S0191 | Winexe | Open Source | Remote command execution for Windows systems |
| S0160 | Certutil | LotL | Payload download and Base64 encoding/ decoding |
| S1205 | cipher.exe | LotL | Secure file wiping |
| S0193 | Forfiles | LotL | Indirect command execution |
| S0039 | Net | LotL | Network discovery and account management |

| | | | |
|---|---|---|---|
| S0108 | netsh | LotL | Firewall modification and port forwarding |
| S0645 | Wevtutil | LotL | Event log management and log clearing |

## MOST COMMON TECHNIQUES OF APT44

| ID | | NAME | USAGE |
|---|---|---|---|
| T1566 | .001 | Phishing: Spearphishing Attachment | Sandworm Team has delivered malicious Microsoft Office and ZIP file attachments via spearphishing emails.[31][30][22][1][37][14]<br>During the 2015 Ukraine Electric Power Attack, Sandworm Team obtained their initial foothold into many IT systems using Microsoft Office attachments delivered through phishing emails. [35] |
| T1566 | .002 | Phishing: Spearphishing Link | Sandworm Team has crafted phishing emails containing malicious hyperlinks.[1] |
| T1190 | | Exploit Public-Facing Application | Sandworm Team exploits public-facing applications for initial access and to acquire infrastructure, such as exploitation of the EXIM mail transfer agent in Linux systems.[27][13] |
| T1003 | .001 | OS Credential Dumping: LSASS Memory | Sandworm Team has used its plainpwd tool, a modified version of Mimikatz, and comsvcs.dll to dump Windows credentials from system memory. [22][26][11]<br>During the 2016 Ukraine Electric Power Attack, Sandworm Team used Mimikatz to capture and use legitimate credentials.[18] |
| T1003 | .003 | OS Credential Dumping: NTDS | Sandworm Team has used ntdsutil.exe to back up the Active Directory database, likely for credential access.[11] |
| T1021 | .002 | Remote Services: SMB/ Windows Admin Shares | Sandworm Team has copied payloads to the ADMIN$ share of remote systems and run net use to connect to network shares.[18][11]<br>During the 2016 Ukraine Electric Power Attack, Sandworm Team utilized net use to connect to network shares.[18] |

| | | | |
|---|---|---|---|
| T0855 | | Unauthorized Command Message | During the 2015 Ukraine Electric Power Attack, Sandworm Team issued unauthorized commands to substation breaks after gaining control of operator workstations and accessing a distribution management system (DMS) application. [35]<br>During the 2022 Ukraine Electric Power Attack, Sandworm Team used the MicroSCADA SCIL-API to specify a set of SCADA instructions, including the sending of unauthorized commands to substation devices.[20] |
| T0846 | | Remote System Discovery | During the 2015 Ukraine Electric Power Attack, Sandworm Team remotely discovered operational assets once on the OT network.[36][15] |
| T1561 | .002 | Disk Wipe: Disk Structure Wipe | Sandworm Team has used the BlackEnergy KillDisk component to corrupt the infected system's master boot record.[30][26] |
| T1486 | | Data Encrypted for Impact | Sandworm Team has used Prestige ransomware to encrypt data at targeted organizations in transportation and related logistics industries in Ukraine and Poland.[11] |

## SOFTWARE USED BY APT44

| ID | NAME | TYPE | DESCRIPTION |
|---|---|---|---|
| S1167 | AcidPour | Custom | Wiper for Linux |
| S1125 | AcidRain | Custom | Wiper for modems/routers |
| S0606 | Bad Rabbit | Custom | Ransomware |
| S0089 | Black Energy | Custom | DDoS and espionage framework |
| S0693 | CaddyWiper | Custom | Wiper |
| S0555 | CHEMISTGAMES | Custom | Espionage malware |
| S0154 | Cobalt Strike | Open Source | PenTest tool (abused) |
| S0687 | Cyclops Blink | Custom | Backdoor for network devices |
| S0363 | Empire | Open Source | Post-exploitation framework |
| S0401 | Exaramel Linux | Custom | Backdoor for Linux |
| S0343 | Exaramel Windows | Custom | Backdoor for Windows |

| | | | |
|---|---|---|---|
| S0342 | GreyEnergy | Custom | Successor to BlackEnergy |
| S0357 | Impacket | Open Source | Toolkit for working with network protocols |
| S0604 | Industroyer | Custom | Attack on industrial systems |
| S1072 | Industroyer2 | Custom | Variant targeting substations |
| S0231 | Invoke-PSImage | Open Source | Hiding PowerShell in .png |
| S1190 | Kapeka | Custom | Backdoor |
| S0607 | KillDisk | Custom | Wiper |
| S0002 | Mimikatz | Open Source | Password stealing |
| S0039 | Net | LotL | Disks mounting, stopping services |
| S0368 | NotPetya | Custom | Pseudo-ransomware / effectively a wiper |
| S0365 | OlympicDestroyer | Custom | Wiper |
| S0598 | P.A.S. Webshell | Custom | Web backdoor |
| S0378 | PoshC2 | Open Source | Powershell C2 framework |
| S1058 | Prestige | Custom | Wiper |
| S0029 | PsExec | LotL | Remote command execution |
| S0195 | SDelete | LotL | Secure file deletion tool |
| S1010 | VPNFilter | Custom | Malware for routers |

# SOURCES


1. OSINT & Phaleristics: Unveiling GRU’s Information Operations Troops (VIO) © CheckFirst 2026
2. Bezek A. 攻心为上：揭秘俄罗斯GRU的心理战“前线部队” [Psychological Operations as a Weapon: Revealing the “Frontline Units” of GRU Psychological Warfare]. Bezek Lab / SecurityLab, March 4, 2021
3. Machulskyi Ye. Russian Information-Psychological Troops: Revelations of a Captured Lieutenant Colonel. Censor.NET, July 28, 2022
4. Main Intelligence Directorate of the Ministry of Defense of Ukraine. Identified Personnel of the Armed Forces of the Russian Federation Fighting in Eastern Ukraine. October 27, 2016
5. shoygu-secretar. Grey Mice in the Central and Eastern Military Districts. LiveJournal, 2020
6. shoygu-secretar. How Can a Dumb Soldier Expose the Activities of a Secret GRU Unit? LiveJournal, 2020
7. OSINT Bees. Who in Russia Is Responsible for PSYOPS. May 24, 2024
8. “Telebachennia Toronto.” Journalists of “Telebachennia Toronto” Exposed a Secret GRU Unit. Media Sapiens, May 4, 2023
9. Meduza. Psy-ops in High Places: Putin’s New Science Adviser to Russia’s National Security Council Is a Military Intelligence Agent Accused of Spreading Disinformation About the Coronavirus. May 17, 2021
10. Paoli C. Russian Hackers Continue Exploiting Microsoft Office Zero-Day After Emergency Patch. February 4, 2026
11. ThreatLabz. APT28 Leverages CVE-2026-21509 in Operation Neusploit. Zscaler, February 3, 2026
12. Trellix. APT28’s Stealthy Multi-Stage Campaign Leveraging CVE-2026-21509 and Cloud C2 Infrastructure
13. Amairy G., Charles M., Sekoia TDR. APT28 Operation Phantom Net Voxel. Sekoia, September 16, 2025
14. UK Government. Profile: GRU Cyber and Hybrid Threat Operations. December 4, 2025
15. The Insider. Google Proved GRU Involvement in New Attacks on U.S. Power Plants and Hacks of Russian Journalists. April 18, 2024
16. Mandiant. Hacktivists Collaborate with GRU-Sponsored APT28. Google Cloud Blog, March 26, 2024
17. Proska K. et al. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Mandiant / Google Cloud Blog, November 9, 2023
18. National Cybersecurity Coordination Center (NCSCC). Cyberattacks, Artillery, Propaganda: A General Overview of the Dimensions of Russian Aggression. January 17, 2023

1. Dobrokhotov R. “Sandworm.” How GRU hackers shut down power plants in Ukraine, hacked the U.S. election commission, and created the most destructive virus in the world. The Insider, October 22, 2020
2. Security Service of Ukraine (SBU). SBU exposes Russian intelligence attempts to penetrate Armed Forces’ planning operations system. August 8, 2023
3. Dobrokhotov R., Shvetsova K. Fraudsters, killers, students: Who makes up the GRU’s team of hacker-provocateurs and why it failed. The Insider, June 2, 2025
4. Microsoft Threat Intelligence. Cadet Blizzard. Microsoft Security Insider
5. National Cyber Security Centre (NCSC). UK and allies uncover Russian military unit carrying out cyber attacks and digital sabotage for the first time. September 5, 2024
6. Dobrokhotov R., Shvetsova K. Hidden Bear: The GRU hackers of Russia’s most notorious kill squad. The Insider, May 31, 2025
7. CISA, NSA, FBI, NCSC-UK, BND, BSI, BfV, VZ, NÚKIB, BIS, ABW, SKW, DC3, USCYBERCOM, ASD’s ACSC, CCCS, DDIS, EFIS, NCSC-EE, ANSSI, MIVD. Russian GRU Targeting Western Logistics Entities and Technology Companies. May 20, 2025
8. Brandefense CTI Analyst Team. SandWorm APT Group Cyber Intelligence Report (Summary). October 19, 2022
9. Rewards for Justice (U.S. Department of State). GRU Officers — Unit 29155
10. Council of the European Union. Council Decision (CFSP) 2025/171 of 27 January 2025 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, January 27, 2025
11. Council of the European Union. Council Decision (CFSP) 2024/3174 of 16 December 2024 amending Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia’s destabilising activities. Official Journal of the European Union, December 16, 2024
12. Cheravitch J. The Role of Russia’s Military in Information Confrontation. CNA, June 2021