NOVACAINE.
ARCANA IMPERII

PUBLICATION PAPER

INSIGHT Opening Insights into Public Security and Information

December 12, 2024

About This Report

This is a data & fact-based research designed to open up insights on important issues!

Important Notes

Not an institutional opinion or official report! All content is purely the author's perspective based on research.

ISTOCK

FiveBears Operations - Russian Hackers Group in the Kremlin

Candra Ihsan

This article examines cyber operations conducted by Advanced Persistent Threat (APT) groups affiliated with Russian intelligence agencies, including the GRU, SVR, and FSB. Since the 1990s, Russia has used cyber operations for espionage, sabotage, and global influence. Key groups such as Fancy Bear (APT28), Cozy Bear (APT29), Venomous Bear (Turla), Energetic Bear (Dragonfly), and Voodoo Bear (Sandworm) target governments, the energy sector, critical infrastructure, and political organizations. Their attacks include the 2016 US election hack, the NotPetya destructive malware, and the infiltration of global energy networks. With sophisticated techniques and false flag strategies, these groups are difficult to identify and continue to evolve. Their operations support Russia's foreign policy and strengthen its geopolitical position. This study highlights how Russian cyber threats impact global security and emphasizes the need for an effective response to increasingly complex attacks.

Origin and Connectivity with Intelligence Agencies

In the 1990s, Russia carried out various dangerous cyber operations, ranging from espionage (stealing classified information) to sabotage (destroying or disrupting systems). One of the earliest well-known operations was the Moonlight Maze attack in 1996, which marked the beginning of a complex cyber operations network linked to Russia. Today, Russian government-backed threat groups form an organized and highly skilled network, conducting operations on a global scale. Their objectives include supporting Russia's foreign policy, obstructing adversaries, preventing conflict escalation, and assisting Russia in strategically managing conflicts. These cyber operations have become a crucial element of Russia's global power strategy.

However, identifying these groups is a major challenge. They frequently change their tools and attack methods or even share tools with other groups. As a result, information about these operations can change over time based on new findings. Cybersecurity firms also often use different names for the same groups, making it difficult to align reports about them. Despite this, these groups remain a serious and evolving threat. [1]

Fancy Bear

A notorious hacking group is strongly suspected of operating under the Russian Main Intelligence Directorate (GRU), specifically Unit GTsSS 26165 [2] ; [3].. This group gained global attention for its involvement in disrupting the 2016 U.S. presidential election. Fancy Bear has significant resources and is known for its persistence in carrying out cyber attacks. Beyond the United States, the group has also conducted dangerous operations in Europe and has recently expanded its targets to the East [4].

Fancy Bear has been active since at least 2004, making it one of the most experienced cyber actors. It is also known by various other names used by cybersecurity firms, including Sofacy, APT28, Sednit, Pawn Storm, Group 74, Tsar Team, Strontium, Swallowtail, SIG40, Grizzly Steppe, TG-4127, and SNAKEMACKEREL. These names frequently appear in reports documenting their activities, reflecting the extensive reach of Fancy Bear's cyber operations.

Specific targets: governments, political parties, anti-chemical weapons organizations, anti-doping organizations, the energy sector, and educational institutions.

Figure 1. FBI wanted list of Russian military intelligence officers connected to the GRU. Source: Federal Bureau of Investigation

Cozy Bear

Just like Fancy Bear, this hacking group is highly organized, well-resourced, and deeply dedicated, with strong ties to the Russian Foreign Intelligence Service (SVR) [5]. Cozy Bear's primary focus is cyber espionage—gathering intelligence from around the world to support Russia's security policies. The group has been linked to the Russian government since at least 2008 [2].

One of Cozy Bear's defining characteristics is its persistence in trying to regain access to specific target networks, even after losing operational control [5].

It is known by various other names, depending on the source or cybersecurity company referencing the group. Some alternative names for Cozy Bear include APT29, Dukes, Group 100, Cozy Duke, EuroAPT, CozyCar, Cozer, Minidionis, SeaDuke, and Hammer Toss.

Specific targets: governments, research institutions, think tanks, and political organizations.

Venomous Bear

Venomous Bear, also known by many other names such as Turla Group, Snake, and Waterbug, is a highly motivated cyber actor group focused on gathering diplomatic intelligence. The group is strongly suspected of being supported by Signals Intelligence (SIGINT) capabilities linked to the Russian Federal Security Service (FSB) [3].

Active since at least 2004 [2], Venomous Bear is known for its exceptional adaptability, employing new and advanced techniques to maintain its operational security [6].

With various aliases such as Group 88, Krypton, Uroburos, and ITG12, the group continues to demonstrate flexibility and innovation in the world of cyber espionage, making it one of the most difficult threats to detect in cyberspace.

Specific Targets: government, military, educational institutions, research institutions, space sector, telecommunications, and pharmaceutical companies.

Energetic Bear

This group of cyber actors is highly sophisticated and is suspected of operating under the control of Centre 16 belonging to the FSB, Russia's intelligence agency. This group is known for targeting sectors that are considered strategic for the national interest. Its main targets include energy installations, oil and natural gas resources in the Middle East, as well as military communications equipment. Energetic Bear has been active since at least the end of 2010, showing a consistent and well-planned pattern of operations.[7] ; [3] ; [8] ; [9]

The group is also known by various other names, including Dragonfly, Crouching Yeti, Group 24, Koala Team, Berserk Bear, Anger Bear, Dymalloy, Havex, PEACEPIPE, Fertger, TEMP. Isotope, and ALLANITE.

Specific Targets: government, aviation sector, energy, industrial control systems, and critical infrastructure.

Figure 2. The FBI's list of wanted Russian hackers connected to the FSB's Center is 16. Federal Bureau of Investigation

Voodo Bear

One of the most notorious Advanced Persistent Threat (APT) groups from Russia, known for its attacks on

critical infrastructure. The group gained widespread attention for its involvement in attacks on Ukraine's power grid in 2015 and the NotPetya cyberattack in 2017. Voodoo Bear is suspected to be a cyber unit operating under the control of the GRU, Russia's military intelligence agency, precisely from the Main Centre for Special Technologies (GTsST) Unit 74455. The group has been active since at least 2009 and carries out sophisticated operations, ranging from espionage to cyberattacks of a destructive nature.[10] ; [2]

In March 2022, human rights investigators from the UC Berkeley School of Law asked the International Criminal Court (ICC) in The Hague to consider the group's operations as an attack on war, particularly related to the conflict in Ukraine.[11]

The group is known by various other names, including the Sandworm Team, TEMP. Noble, Electrum, TeleBots, Black Energy, Hades, and many more.

Specific Targets: Ukraine's Energy Sector, government, anti-chemical weapons organizations, political parties and campaigns, and critical infrastructure.

Russian APT Bear Group

The Five Bear APT (Advanced Persistent Threat) group often changes the tools they use, shares tools with other groups, or performs false flag operations to avoid tracking and attribution. This makes it difficult to ascertain who is responsible for a particular cyberattack. [2]

STRATEGIC PURPOSE :

Targeting Attack

Russian APT groups have proven capable of carrying out attacks that disrupt critical infrastructure belonging to their opponents. These attacks often use malware designed to target industrial control systems (ICS). If these attacks are successful, they can gain access to protected systems, allowing for actions that are destructive. In addition, the Russian APT group has the ability to survive in networks they have already hacked undetected for long periods of time, using a variety of techniques to gain early access.[3]

Espionage Operation

The Russian-affiliated APT group is also involved in cyber espionage targeting the energy, aviation, transportation, health, and telecommunications sectors. The operation is coordinated by Russia's intelligence agencies to serve a variety of purposes, from developing new cyber capabilities to supporting Russia's foreign policy.[3]

Influence Operation

In addition to direct attacks, Russian government-backed cyber actors are also seeking to undermine confidence in Western democratic systems. They use secret online media and fake news outlets to spread disinformation. In addition, the APT group conducts operations targeting government agencies, influencing national elections, and leaking sensitive information such as medical records to create instability.[3]

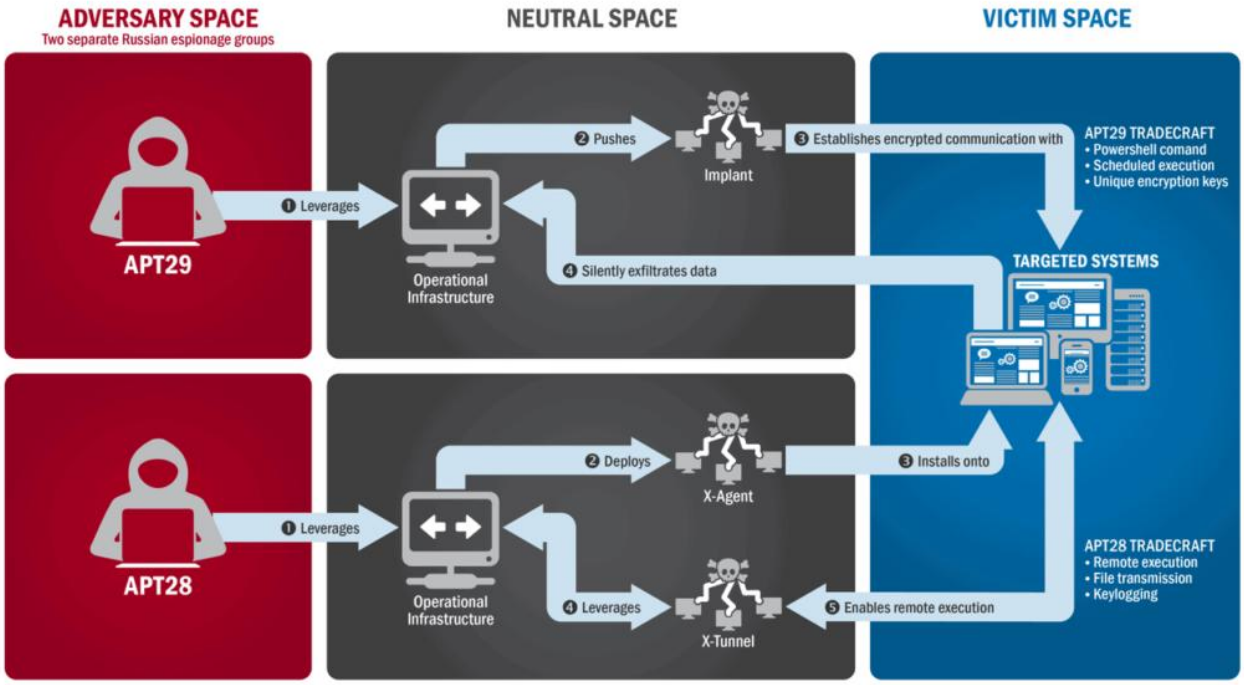

Figure 3. Diagram from the US-Cert Report on APT28 and APT29 (aka Grizzly Steppe)-Image: Wikicommons

FIVE BEAR ACTION:

NotPetya Attack

In 2017, Ukraine's financial institutions and government were targeted by major cyberattacks carried out by Russian government-backed actors. This attack uses the NotPetya malware, which is known to be one of the fastest-spreading malware. By utilizing the EternalBlue and Mimikatz tools, this malware is able to bypass security gaps in Windows systems, even on patched systems. Once one device is infected, the malware spreads very quickly, deleting important data on the victim's computer and rendering the device unusable.

What sets NotPetya apart is its purely destructive nature—this malware is not designed to be decrypted or recovered, thus making it more of a weapon of destruction than a tool for data theft. [10] ; [12]

Global Energy Sector Intrusion Campaign

Between 2011 and 2018, cyber actors backed by the Russian government launched a massive attack campaign targeting the international energy sector network. In these attacks, they mainly conduct reconnaissance to study the target systems and launch malware specifically designed to attack Industrial Control Systems (ICS), which are systems that control critical operations in the energy sector. These attacks aim to disrupt, steal information, or even damage the energy infrastructure that is the backbone of many countries.[13]

Ukraine Power Grid Attacks

In 2015 and 2016, the Russian government-backed APT (Advanced Persistent Threat) group carried out cyberattacks targeting energy distribution companies in Ukraine in 2015, and electricity transmission companies in 2016. As a result of this attack, there were power outages in some areas, and many infected

computers became unusable. These attacks demonstrate the group's ability to disrupt critical infrastructure such as power grids, which has a direct impact on people's lives and the stability of the country.[13]

US Presidential Election Hack

In 2016, a network belonging to the Democratic National Committee (DNC) in the United States was targeted by a spear phishing attack, which is a cyberattack that targets a specific individual or organization through a fake email that looks convincing. This attack succeeded in giving the perpetrators access to documents related to the election. This incident is one example of how cyberattacks can be used to influence the political process. [14] ; [3]

Reference

[1] O. o. t. D. o. N. Intelligence, "ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY," 2021.

[2] A. Cristaldi, "APTMAP," Github, [Online]. Available: https://andreacristaldi.github.io/APTmap/#34.

[3] C. M. Centre, "SUBSTANTIVE REVISION: Russia: Cyber Threat Overview," OFFICE of INTELLIGENCE AND ANALYSIS, 2022.

[4] Great, "Masha and these Bears," SecureList, 09 March 2018. [Online]. Available: https://securelist.com/masha-and-these-bears/84311/.

[5] C. Strike, "Cozy Bear," CrowdStrike, [Online]. Available: https://www.crowdstrike.com/adversaries/cozy-bear/.

[6] C. Strike, "Venomous Bear," CrowdStrike, [Online]. Available: https://www.crowdstrike.com/adversaries/venomous-bear/.

[7] C. R. Service, "Russian Cyber Units," 2022.

[8] D. B. B. B. B. Z. C. J. E. K. B. M. M. M. K. A. J. C. P. H. B. I. A. G. D. A. C. F. E. S. F. E. O. Z. G. W. Pasquale Stirparo, "APT Groups and Operations," 2023. [Online]. Available: https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml.

[9] K. L. G. R. a. A. Team, "Energetic Bear — Crouching Yeti," Kapersky, 2018.

[10] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[11] A. Greenberg, "The Case for War Crimes Charges Against Russia's Sandworm Hackers," Wired, 2022. [Online]. Available: https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/.

[12] E. Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes," Washington Post, 2018. [Online]. Available: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[13] A. C. D. Agency, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," 01 03 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a.

[14] D. P. Office, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," Homeland Security, 07 October 2016. [Online]. Available: https://www.dhs.gov/archive/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.