



| Flash |

Anonymous Russia Announces War Against NATO

F-2023-12-14a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Ransomware, Deep and Dark
Web

December 14, 2023

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 10:00 AM (EST) on December 14, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Anonymous Russia Announces War Against NATO

› Key Findings

- On December 14, 2023, the pro-Russian hacktivist collective known as Anonymous Russia announced in its Telegram channel that it is preparing for a cyber war against NATO.
- Anonymous Russia is known for its politically-motivated targeting; it typically conducts defacements and data leaks and launches Distributed Denial of Service (DDoS) attacks against pro-Ukrainian targets.
- The collective is unlikely to have the capability to conduct a highly-disruptive campaign against NATO targets of critical value, and any attacks are likely to have limited operational impact. However, ZeroFox cannot rule out that campaigns against NATO-aligned countries or entities could involve collaboration with more capable hacktivist groups.

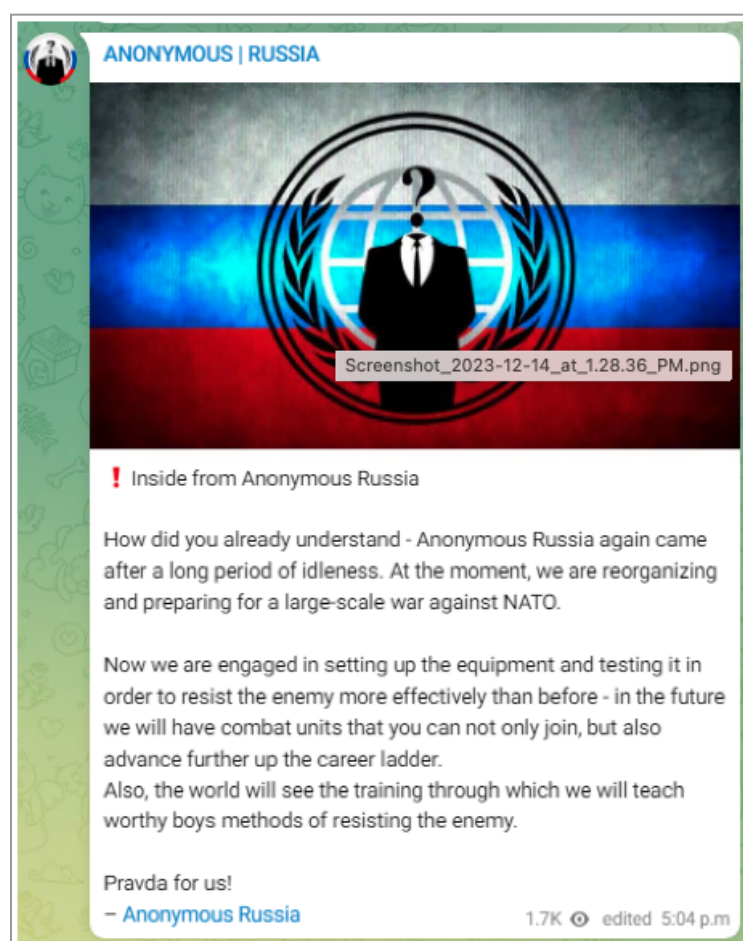
Details

On December 14, 2023, the pro-Russian hacktivist collective known as Anonymous Russia announced in its Telegram channel that it is preparing for a cyber war against NATO. The group, which claims to be resuming operations after a period of inactivity, has a history

of collaborating with other pro-Russian online collectives to compromise perceived pro-Ukrainian targets.

In its post, Anonymous Russia stated that it is currently setting up and testing equipment ahead of launching a large-scale war against NATO targets.

- No specific entities were named directly in the post.
- The post indicates the group is active canvassing for community support of its operations.



Anonymous Russia announces that it is preparing for a cyber war against NATO

Source: ZeroFox Collections

Anonymous Russia is known for its politically-motivated targeting, typically conducting defacements and data leaks and launching Distributed Denial of Service (DDoS) attacks

against its victims. The collective very likely seeks to target NATO-aligned entities due to their political and military support for Ukraine. The collective has a history of collaborating with other pro-Russian hacktivist groups, including Killnet, NoName057(16), XakNet Team, and Cyber Army of Russia.

- The group is not linked to the wider Anonymous hacking collective, which has previously announced its support for Ukraine.
- In April 2023, KillNet's leader, "Killmilk", doxxed the alleged head of Anonymous Russia, "Raty", sharing a passport photo that revealed his name and that he was an 18-year-old Belarusian citizen; Raty was later arrested. Anonymous Russia's Telegram group was wiped, and Killmilk announced the appointment of a new head of Anonymous Russia, "Radis."

Anonymous Russia is unlikely to have the capability to conduct a sophisticated campaign against NATO targets. Despite its relaunch, Anonymous Russia's campaigns are unlikely to result in mass or prolonged outages to infrastructure and are most likely to be limited to minor operational impacts from DDoS attacks and website defacements.

- The group's limited capabilities notwithstanding, ZeroFox cannot rule out that campaigns against NATO-aligned countries could involve collaboration with more capable hacktivist groups.

Recommendations

- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new Anonymous Russia developments.
- Configure the ZeroFox Intelligence Platform to monitor for current mentions of your organization on Anonymous Russia's Telegram channel.
- Beware of spikes in traffic, suspicious emails, and/or unauthorized access to the active directory.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%