



| Flash |

Pro-Russia Actors Threaten Paris Olympics

F-2024-07-30a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Vulnerability Exploitation

July 30, 2024

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 9:00 AM (EST) on July 30, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Pro-Russia Actors Threaten Paris Olympics

› Key Findings

- The 2024 Olympics, scheduled to be held from July 26 to August 11 in Paris, France, is facing and likely will continue to face cyberattacks—primarily from politically motivated actors.
- Pro-Russian hacktivists are likely to conduct low impact attacks targeting Olympics-related events and states that oppose Russia's participation in the Games.
- Russian-aligned actors will likely try to undermine the International Olympic Committee (IOC) via disinformation campaigns. These efforts may result in disruption to the event, dissuade spectators from attending, and create fear among attendees and athletes, leading to reputational damage of the host (France), the IOC, and, by extension, the West.
- Malicious Pro-Russian cyber activities are likely part of a broader strategic initiative seeking to undermine both France's security, credibility, and ability to host such a large-scale international event, as well as that of the IOC.

Details

ZeroFox has observed politically-motivated, primarily pro-Russian threat actors overtly threatening the Paris 2024 Olympic Games in the run-up to the event. The majority of these are hacktivist collectives aiming to disrupt the event by leveraging distributed denial-of-service (DDoS) attacks or discredit the Olympics' reputation via disinformation campaigns. The media, public, and government attention to the Games also makes it an attractive target for malicious cyber actors intending to cause disruption and gain prominence—both for themselves and for their political cause.

Various pro-Russia hacktivist groups are likely to conduct low impact attacks targeting Paris 2024. This is in addition to threats posed by notorious state-sponsored Russian advanced persistent threat actors (APTs), including APT 28 (aka Fancy Bear, STRONTIUM, and Forest Blizzard) and APT 29 (aka NOBELIUM, Office Monkeys, StellarParticle, UNC2452, and Midnight Blizzard). Both categories of actors are likely to be motivated, in varying degrees, to target the Olympics to advance the geopolitical interests of Russia.

- Russia has been officially banned from participating in the games by the IOC due to its role in the Russia-Ukraine war. The Russian Olympic Committee (ROC) has absorbed several regional sports organizations in Ukraine (Donetsk, Kherson, Luhansk, and Zaporizhzhia), which were previously governed by the National Olympic Committee (NOC) of Ukraine. In adherence with the Olympic Charter, the ROC is banned from participating in the Paris 2024 Olympic games for violating the territorial integrity of Ukraine's NOC.¹ (After Russia was barred from previous Olympics competitions due to accusations of a state-backed doping scheme, Russian athletes were still allowed to compete under other labels like "ROC" and "Olympic Athletes from Russia."²³)

¹

[hXXps://olympics\[.\]com/ioc/news/ioc-executive-board-suspends-russian-olympic-committee-with-immediate-effect](https://olympics.com/ioc/news/ioc-executive-board-suspends-russian-olympic-committee-with-immediate-effect)

²

[hXXps://www.nbcwashington\[.\]com/paris-2024-summer-olympics/russia-name-roc-ain-2024-olympics/3647116/](https://www.nbcwashington.com/paris-2024-summer-olympics/russia-name-roc-ain-2024-olympics/3647116/)

³

[hXXps://abcnews.go\[.\]com/International/russian-team-barred-competing-winter-olympics/story?id=51582308](https://abcnews.go.com/International/russian-team-barred-competing-winter-olympics/story?id=51582308)

- In 2016, the World Anti-Doping Agency (WADA) confirmed its database was hacked by a cyber espionage threat group linked to Russian intelligence, two years after detailed allegations were made tying Russia to a doping scheme.⁴
- France, the host of this year's Olympics and a founding member of NATO, has condemned Russia's war in Ukraine "in the strongest possible terms."⁵ Additionally, France has delivered EUR 2.615 billion (USD 2.76 billion) in military aid and contributed EUR 1.2 billion (USD 1.28 billion) to the European Peace Facility (EPF), totaling over EUR 3.8 billion (USD 4.04 billion). France also trained nearly 10,000 Ukrainian soldiers in Poland and France.⁶
- Other NATO members and Games-participating countries, such as the United States and the United Kingdom, have also consistently criticized Russia's invasion of Ukraine and pushed for Russia's exclusion from the Olympics.⁷

Malicious pro-Russian cyber activities are likely part of a broader strategic initiative seeking to undermine both the IOC and France's security, credibility, and ability to host such a large-scale international event.

- On July 24, 2024, police announced they had arrested a Russian national days earlier for a plot to "destabilize" France. The suspect reportedly passed information to Russian intelligence that could be used to conduct pro-Russian operations during the Olympics.
- Prior to that, following President Macron's suggestion that French forces could be deployed to Ukraine, a number of coffins which mimicked dead French soldiers were found at the base of the Eiffel Tower. French authorities have tied this, as well as mass graffiti across Paris depicting the Star of David, to Russia.⁸

4

[hXXps://www.nbcnews\[.\]com/storyline/2016-rio-summer-olympics/russian-hackers-post-medical-files-biles-serena-williams-n647571](https://www.nbcnews.com/storyline/2016-rio-summer-olympics/russian-hackers-post-medical-files-biles-serena-williams-n647571)

5

[hXXps://www.nato\[.\]int/cps/en/natohq/topics_192648.htm#:~:text=What%20is%20NATO%20doing%20to,both%20sides%20of%20the%20Atlantic.](https://www.nato.int/cps/en/natohq/topics_192648.htm#:~:text=What%20is%20NATO%20doing%20to,both%20sides%20of%20the%20Atlantic.)

⁶ [hXXps://www.defense.gouv\[.\]fr/en/news/french-military-equipment-delivered-ukraine](https://www.defense.gouv.fr/en/news/french-military-equipment-delivered-ukraine)

7

[hXXps://www.usnews\[.\]com/news/best-countries/articles/these-countries-have-committed-the-most-aid-to-ukraine](https://www.usnews.com/news/best-countries/articles/these-countries-have-committed-the-most-aid-to-ukraine)

⁸ [hXXps://www.bbc\[.\]com/news/articles/cdlj7kg2nk0o](https://www.bbc.com/news/articles/cdlj7kg2nk0o)

ZeroFox Intelligence has observed at least two instances of pro-Russian threat actors steering their activities to target the Olympics, as detailed below.

Hacktivist group “Cyber Army of Russia Reborn” (CARR) is one of the primary threat groups claiming to be preparing to disrupt the online infrastructure of the Olympics. On June 23, the group announced its plans to target France with continued DDoS campaigns with the support of other actors, including “Noname057(16),” “Hacknet,” “Cyber Dragon,” and “UserSec.”⁹ The collective has also targeted the French Film Festival as a part of its ongoing efforts to target the Olympics. While CARR has conducted multiple high-profile attacks in recent years, they are typically low impact and cause temporary disruptions to websites; the threat actor is unlikely to have the capability to significantly disrupt the Olympic Games.

- CARR was created by GRU-controlled APT “Sandworm,” and its activities appear to align with Russia’s geopolitical goals.¹⁰
- CARR is notable for targeting water and wastewater facilities across the United States.¹¹

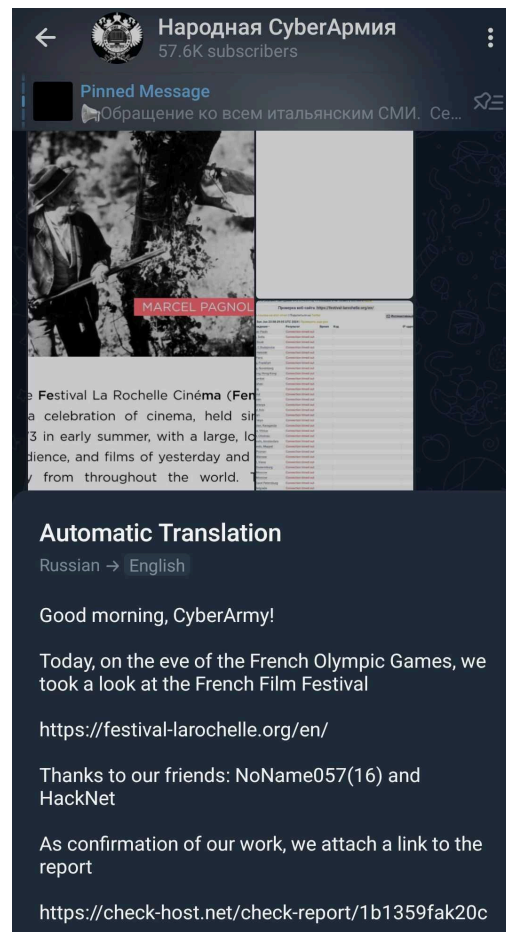
⁹ [https://cloud.zerofox\[.\]com/intelligence/advanced_dark_web/66297](https://cloud.zerofox[.]com/intelligence/advanced_dark_web/66297)

¹⁰

[hXXps://www.cpomagazine\[.\]com/cyber-security/state-sponsored-russian-hackers-linked-to-breach-of-texas-water-treatment-plant/](https://www.cpomagazine[.]com/cyber-security/state-sponsored-russian-hackers-linked-to-breach-of-texas-water-treatment-plant/)

¹¹

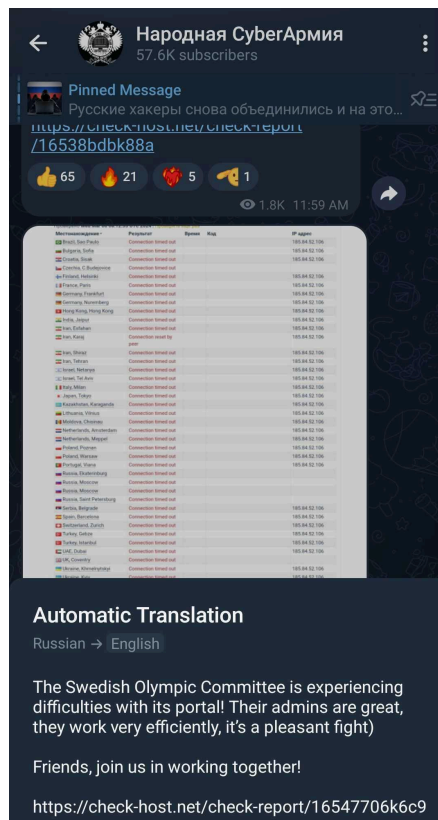
[hXXps://www.cisa\[.\]gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity](https://www.cisa[.]gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity)



CARR Announces Attack Against French Film Festival

Source: ZeroFox Intelligence

- The group has targeted the Swedish Olympic Committee website in a DDoS attack, uploading images as proof of timeouts. The attack demonstrated CARR's willingness to potentially expand its attacks to various Olympic-related entities.



CARR Announces DDoS Attacks Targeting Swedish Olympic Website

Source: ZeroFox Intelligence

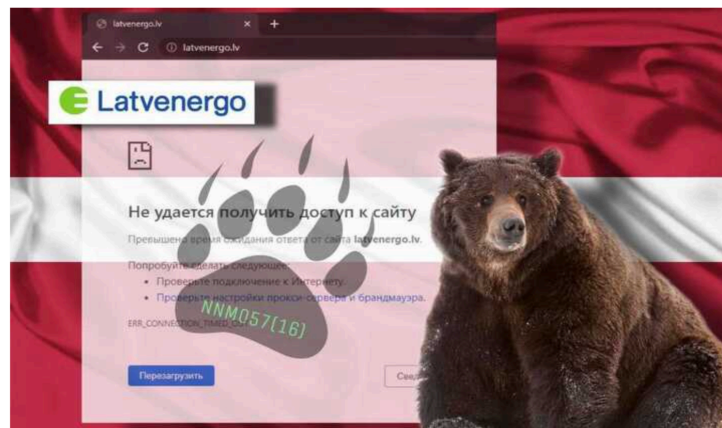
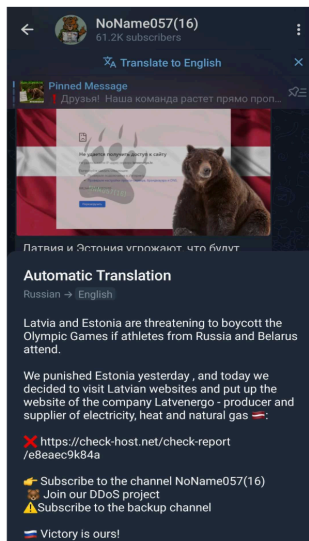
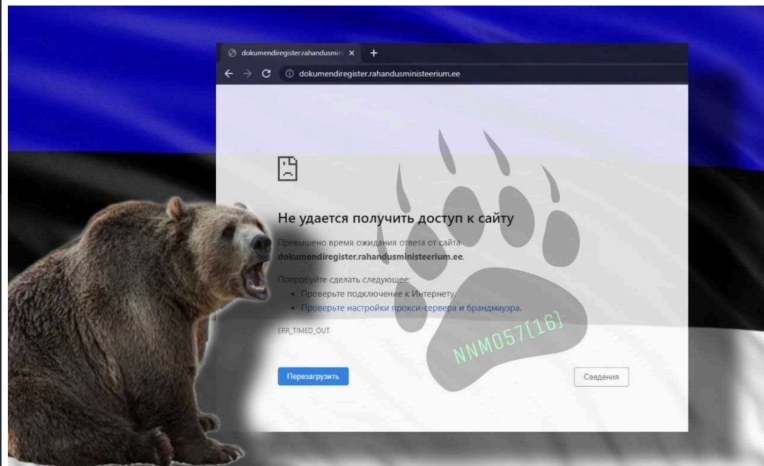
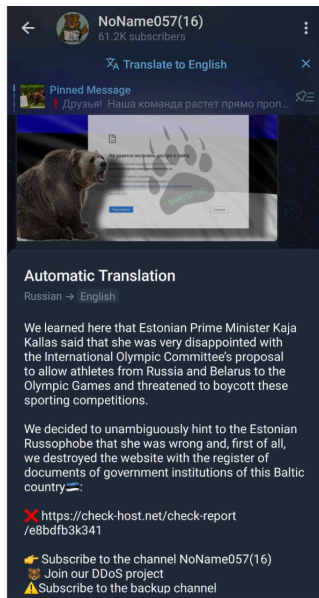
There is also a likely increased threat from another pro-Russian hacktivist group, NoName057(16), that has previously targeted U.S. critical infrastructure—including a wastewater plant in Indiana. The group has mainly conducted DDoS attacks against entities from countries that have opposed Russian interests, including Russia’s participation in the Olympics.

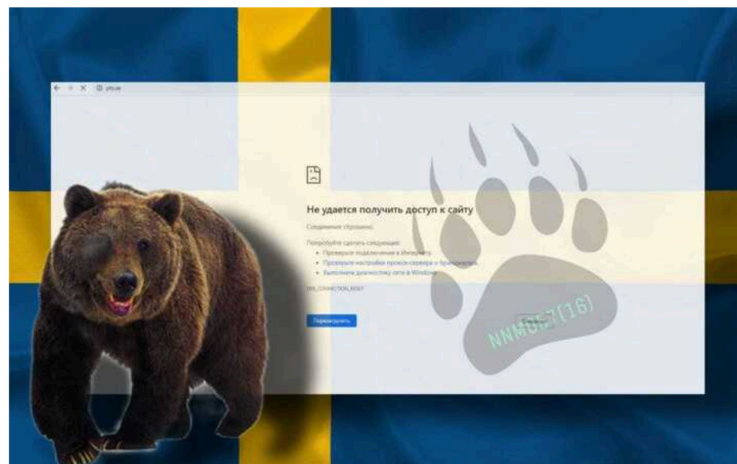
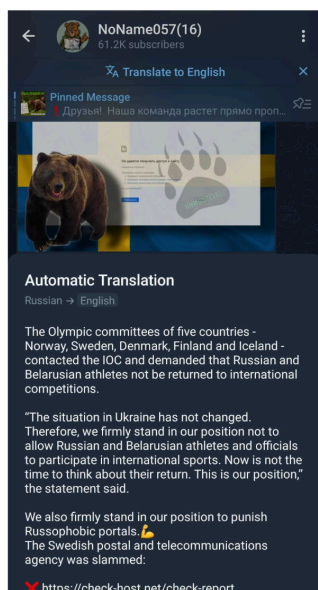
- In February 2023, NoName057(16) targeted a website containing the registry of Estonia and Latvenergo's government documents, a state-owned electric utility company in Latvia, and a Swedish postal and telecommunications agency. The adversary stated its motive was anti-Russian sentiments from the targeted countries.

Flash | Pro-Russia Actors Threaten Paris Olympics

F-2024-07-30a

TLP:CLEAR





NoName 057(16) Announces Attacks Targeting Websites from Sweden, Estonia, and Latvenergo

Source: ZeroFox Intelligence

In addition to the direct threat of DDoS attacks, the Paris Olympics is very likely to be indirectly targeted by disinformation campaigns and related data breach incidents. The most impactful threat is likely to be from Russian state-linked threat actors.

- In early June 2024, a Kremlin-linked group called “Storm-1679” released a feature-length film, *Olympics Has Fallen*, using artificial intelligence (AI) to impersonate Tom Cruise and discredit the IOC.¹²
- Storm-1679 and “Storm-1099” have reportedly been devising Olympic-specific disinformation campaigns since June 2023. These efforts are likely to invite more state-linked activity targeting the IOC and the Olympics, in an attempt to undermine the legitimacy of the committee and French security forces.¹³

More pro-Russian hackers are likely to follow suit and conduct DDoS attacks, paralyze

¹²

[hXXps://www.theguardian\[.\]com/technology/article/2024/jun/03/russia-paris-olympics-deepfake-to-m-cruise-video](https://www.theguardian.com/technology/article/2024/jun/03/russia-paris-olympics-deepfake-to-m-cruise-video)

¹³

[hXXps://www.reuters\[.\]com/technology/russian-disinformation-campaign-takes-aim-paris-olympics-microsoft-says-2024-06-03/](https://www.reuters.com/technology/russian-disinformation-campaign-takes-aim-paris-olympics-microsoft-says-2024-06-03/)

key systems, spread disinformation, and carry out phishing schemes targeting Olympic officials, participants, and attendees. These attacks are intended to be a nuisance in general, causing inconvenience to people and attempting to harass the authorities. Hacktivists will most likely attempt to press their geopolitical agendas through these attacks, attempt to undermine the legitimacy of the IOC, and damage the reputation of the Olympics. Disinformation campaigns also have the potential to negatively influence audience turn-out at the Paris 2024 events.

| Recommendations

- Implement secure password policies with phishing-resistant, multi-factor authentication (MFA), complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of ransomware and digital extortion (R&DE threats); their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.

| 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%