ZEROFOX INTELLIGENCE

Flash

Sabotage and Cyber Disruptions at Milano Olympics

F-2026-02-13a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical, Physical Security, DDW

February 13, 2026

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 11:45 AM (EST) on February 13, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Sabotage and Cyber Disruptions at Milano Olympics

| Key Findings

- The Russian Federation has a history of targeting the Olympics with cyberattacks as revenge for its formal exclusion from the Games (such as in the Paris 2024 Summer Olympics). With Russian athletes once again slated to compete as Individual Neutral Athletes rather than represent the country and the added factor of Italy's continued support for Ukraine,[1] Russia-aligned hackers are likely to continue targeting the cyber infrastructure of the 2026 Winter Olympics.

- Pro-Russian hacktivists are very likely to continue conducting low-impact attacks targeting Olympics-related events and states that oppose Russia's participation in the Games.

- Protests, travel disruptions, and acts of sabotage targeting transportation infrastructure have also taken place and are likely to continue through the Games.

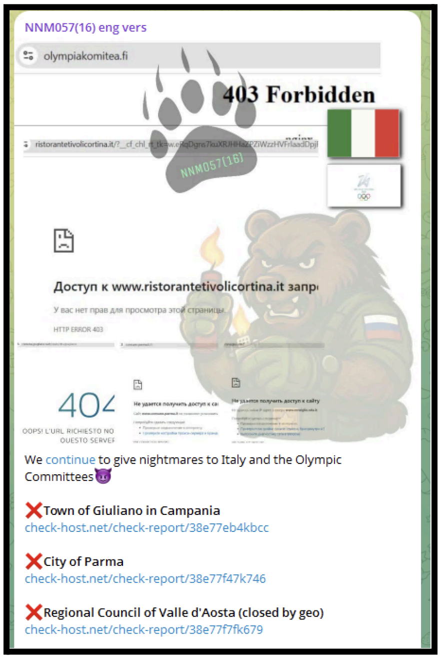
[1] hXXps://www.themoscowtimes[.]com/2026/02/12/at-milan-cortina-winter-olympics-russian-athletes-are-a-diminished-presence-a91929.

- There is a roughly even chance that these efforts will result in minor disruptions to the event, dissuade spectators from attending, and lead to reputational damage for the host and the International Olympic Committee (IOC).

Details

ZeroFox has observed politically motivated, primarily pro-Russian threat actors overtly targeting the 2026 Winter Olympics since they began. Z-Pentest and NoName057(16)—two of the most active pro-Russian hacktivist groups—have claimed responsibility for the majority of these attacks.[2] These groups employ easily disseminated and replicated tactics, techniques, and procedures (TTPs), which enable widespread adoption and a consistently high rate of attack.

- Both Z-Pentest and NoName057(16) have largely stuck to their preferred attack types. Z-Pentest has primarily carried out intrusions into operational technology (OT) or industrial control systems (ICS), while NoName057(16) has launched dozens of distributed denial-of-service (DDoS) attacks.


olympiakomitea.fi
403 Forbidden
ristorantetivolicortina.it/?__cf_chl_rt_tk=w.eRqDgns7kuXRJHHaZPZiWzzHVFrlaadDpjI
NNM057(16)
Доступ к www.ristorantetivolicortina.it запр
У вас нет прав для просмотра этой страницы.
HTTP ERROR 403
404
OOPS! L'URL RICHIESTO NO
QUESTO SERVER
Не удается получить доступ к са
Не удается получить доступ к сайту

NNM057(16) eng vers

We continue to give nightmares to Italy and the Olympic Committees😈

❌Town of Giuliano in Campania
check-host.net/check-report/38e77eb4kbcc

❌City of Parma
check-host.net/check-report/38e77f47k746

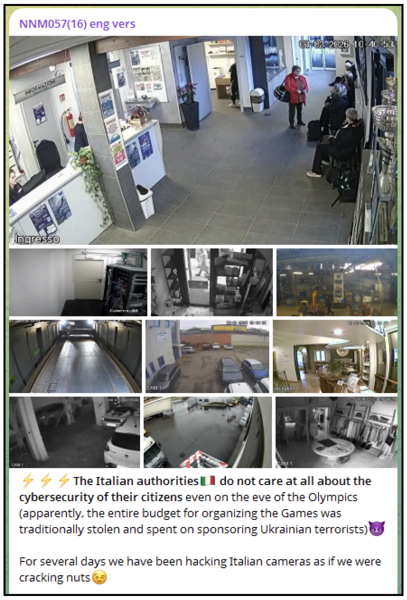
❌Regional Council of Valle d'Aosta (closed by geo)
check-host.net/check-report/38e77f7fk679

NoName057(16) claims to have targeted an Italian municipality website

Source: ZeroFox Intelligence

[2] hXXps://t[.]me/zpentestalliance/1058

Prior to the Olympics, several pro-Russian hacktivist groups claimed access to various CCTV or security camera systems in target countries, which NoName057(16) has replicated during the Olympics.[3] ZeroFox has observed the group posting photos claiming access to various cameras throughout Italy. These cameras do not appear to be civilian security cameras that are operationally significant, which suggests this attack vector is likely intended as an intimidation tactic.


NNM057(16) eng vers

⚡⚡⚡**The Italian authorities🇮🇹 do not care at all about the cybersecurity of their citizens** even on the eve of the Olympics (apparently, the entire budget for organizing the Games was traditionally stolen and spent on sponsoring Ukrainian terrorists)😈

For several days we have been hacking Italian cameras as if we were cracking nuts😉

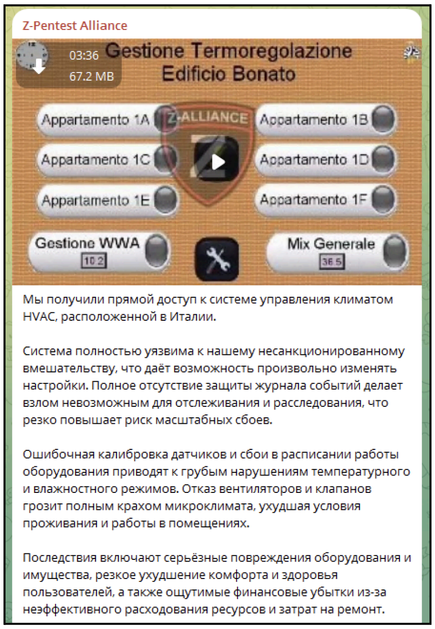
Images from purportedly hacked Italian CCTV cameras during the Olympics on NoName057(16)'s Telegram page

Source: ZeroFox Intelligence

As of reporting, the attacks have been low-impact, which aligns with these groups' level of sophistication. Historically, pro-Russia hacktivist groups have demonstrated limited capabilities and have relied on opportunistic methodology, targeting vulnerable internet-facing devices. Their low level of technical knowledge often results in haphazard attacks in which the threat actor intends to cause damage but cannot anticipate the real impact. Although pro-Russia hacktivists have occasionally damaged critical infrastructure, they often exaggerate their capabilities and the impact of their attacks to garner more attention.[4]

[3] ZeroFox Intelligence
[4] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa25-343a

- Regardless of the true outcome, pro-Russia hacktivist groups post images or screen recordings of the attacks to their social media platforms, boasting and exaggerating the impact to garner increased attention.
- On February 7, Z-Pentest claimed an intrusion into an unidentified Heating, Ventilation and Air Conditioning (HVAC) climate control system "located in Italy".[5] The lack of details suggests this is a low-level target that would not directly impact the Games and reflects Z-Pentest's low sophistication and opportunistic targeting. Rather than conducting a methodical campaign to target the Olympics, Z-Pentest likely used relatively unsophisticated tools to search for vulnerable Virtual Network Computing (VNC) devices in Italy.



Мы получили прямой доступ к системе управления климатом HVAC, расположенной в Италии.

Система полностью уязвима к нашему несанкционированному вмешательству, что даёт возможность произвольно изменять настройки. Полное отсутствие защиты журнала событий делает взлом невозможным для отслеживания и расследования, что резко повышает риск масштабных сбоев.

Ошибочная калибровка датчиков и сбои в расписании работы оборудования приводят к грубым нарушениям температурного и влажностного режимов. Отказ вентиляторов и клапанов грозит полным крахом микроклимата, ухудшая условия проживания и работы в помещениях.

Последствия включают серьёзные повреждения оборудования и имущества, резкое ухудшение комфорта и здоровья пользователей, а также ощутимые финансовые убытки из-за неэффективного расходования ресурсов и затрат на ремонт.

Z-Pentest claims to have hacked an Italian HVAC system

Source: ZeroFox Intelligence

Russia's geopolitical strategies will almost certainly ensure these attacks continue on a frequent basis throughout the remainder of the Games. Russia very likely aims to retaliate against perceived support for Ukraine and the IOC ban on Russian athletes competing.

[5] ZeroFox Intelligence

Italy's status as a NATO member state presents an increased risk to Italian entities, as pro-Russian threat actors very likely seek to embarrass and disrupt supporters of Ukraine.

- In one incident, NoName057(16) claimed to have targeted the websites of Spanish, Lithuanian, and Polish Olympic Committees alongside Sea Aeroporti di Milano.[6]

Protests and Transportation Disruptions

Several smaller anti-Olympics protests took place in the lead-up to the opening ceremony, culminating in a much larger demonstration on February 7 in Milan. In the days before the Games formally began, small groups of demonstrators held protests in towns throughout Italy as the Olympic torch relay passed through. These protests predominantly denounced Israel's participation in the Games and the alleged environmental impact of the Olympics.[7]

- On February 7, the day after the opening ceremony, a much larger protest organized by the Comitato Insostenibili Olimpiadi (CIO) group took place in Milan and saw thousands of participants. While most demonstrators were peaceful, a group of several dozen masked individuals shot firecrackers and threw bottles at police as the march wound down at nightfall.[8] The incident drew condemnation from Italy's prime minister.

Besides protests, the Games have also seen disruptions from the sabotage of railways by self-described anarchist groups.

- On February 7, saboteurs damaged railway infrastructure in three different locations across northern Italy, leading to delays of up to two and a half hours. A self-described anarchist group subsequently claimed responsibility, alleging that the action was precipitated by the passage of a new security law giving police the authority to proactively arrest individuals suspected of planning violent or

[6] hXXps://x[.]com/FalconFeedsio/status/2020835161819202017
[7] hXXps://www.instagram[.]com/p/DTyXUBQiERI/
[8] hXXps://www.aljazeera[.]com/news/2026/2/8/italys-meloni-condemns-anti-olympics-protesters-in-milan

disruptive acts. The group's statement implied that additional actions were likely planned.[9]

- On February 11, the Lecco-Tirano rail line in northern Italy suffered another act of sabotage.[10]

There is a roughly even chance of additional protests against the newly passed security law during the Olympics; these additional protests are almost certain to occur in the coming weeks.

Conclusion

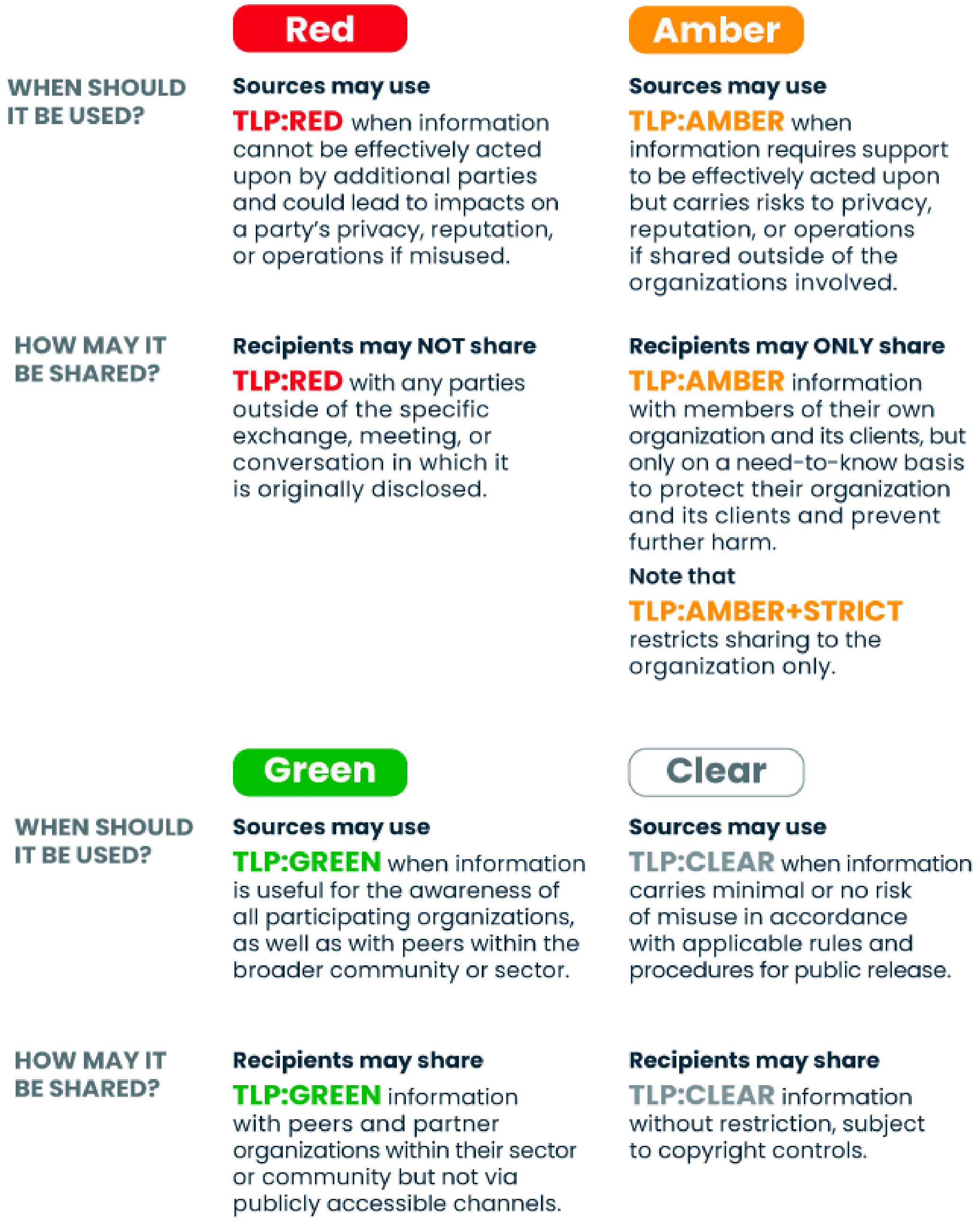
ZeroFox assesses that further efforts to disrupt the Games are very likely. Geopolitically motivated cyber threat actors such as NoName057(16) and Z-Pentest are conducting attacks daily, while transportation strikes have been announced for February 16 and in the days following the Olympics when Olympics-related travel will likely still be occurring.[11] However, authorities have likely prepared for these low-level disruptions, which have occurred at previous Olympic games. However, more sophisticated attacks from state-backed advanced persistent threat groups cannot be ruled out. Meanwhile, deliberate acts of sabotage, like those along northern Italian rail lines are likely to prove more disruptive, as they occur without warning and the damage to physical infrastructure is less easily repaired.

[9] hXXps://www.reuters[.]com/world/anarchists-claim-responsibility-rail-sabotage-during-italy-olympics-2026-02-09/

[10] htXXs://milano.corriere[.]it/notizie/cronaca/26_febbraio_11/olimpiadi-sabotaggio-sulla-linea-ferroviaria-lecco-tirano-che-porta-a-bormio-e-livigno-a-fuoco-con-una-molotov-7-cavi-di-una-7e63cf4f-1e63-4fbf-9867-92d5ce2c9xlk.shtml

[11] hXXps://www.corriere[.]it/economia/trasporti/aerei/26_febbraio_13/scioperi-aerei-del-16-febbraio-e-7-marzo-i-sindacati-non-tornano-indietro-costretti-a-confermare-convocati-troppo-tardi-9e358e6c-36e3-481c-b078-8e8f94815xlk.shtml

Appendix A: Traffic Light Protocol for Information Dissemination

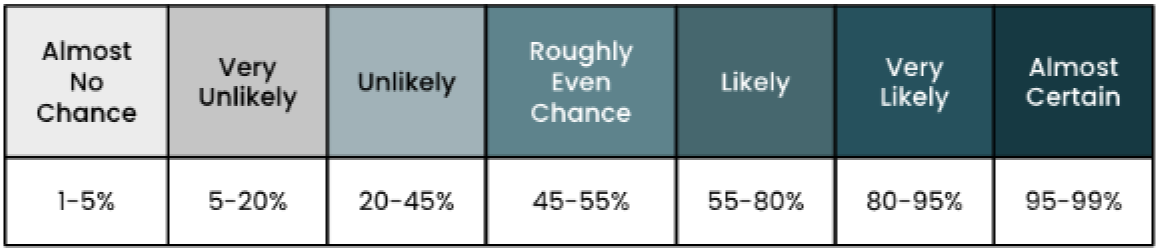


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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%