ZEROFOX INTELLIGENCE

Flash

United Kingdom Issues Alert on Russian-Linked Hacktivism

F-2026-01-22a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Nation-State, Hacktivism

January 22, 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 7:00 AM (EST) on January 22, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | United Kingdom Issues Alert on Russian-Linked Hacktivism

| Key Findings

- On January 19, 2026, the National Cyber Security Centre (NCSC)—a part of the United Kingdom's Government Communications Headquarters (GCHQ)—issued an alert highlighting the persistent targeting of UK organizations by Russian state-aligned hacktivist groups aiming to disrupt networks.
- In the alert, the NCSC highlighted ongoing activity from Russian-linked hacktivist collectives, including coordinated attacks across NATO and European countries.
- On January 12, 2026, ZeroFox observed that "NoName057(16)" and "DarkStorm Team" claimed on their respective official Telegram channels to have conducted distributed denial-of-service (DDoS) attacks targeting multiple organizations based in Poland.
- As tensions between Russia and the West remain, it is very likely that pro-Russia and anti-West hacktivist collectives will continue to target Western institutions throughout 2026.

Details

On January 19, 2026, the NCSC issued an alert highlighting the persistent targeting of UK organizations by Russian state-aligned hacktivist groups aiming to disrupt networks.[1] The alert urges UK organizations—particularly local authorities and operators of critical national infrastructure (CNI)—to strengthen their resilience against denial-of-service (DoS) attacks.

- DoS and DDoS attacks—the most commonly used by Russian hacktivist collectives to cause disruption—typically require relatively low technical skill to conduct. However, they often cause severe financial and operational losses.
- The alert notes that Russian-aligned hacktivist collectives are largely targeting victims whom they perceive support Ukraine and are operating independently of direct state control.

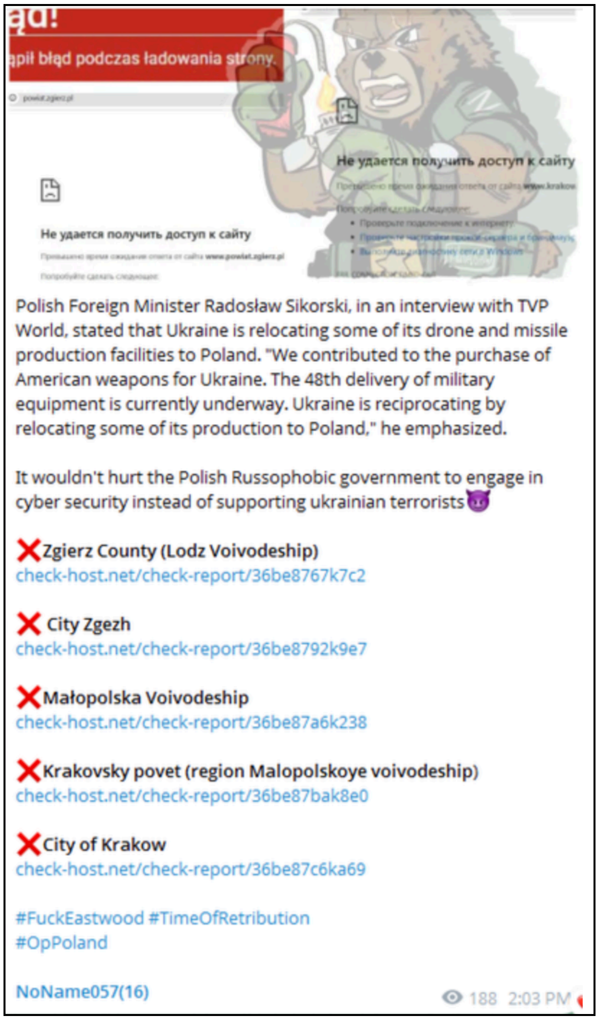
In the alert, the NCSC highlighted ongoing activity from Russian-linked hacktivist collectives (including coordinated attacks across NATO and European countries) and warned of continuous malicious cyber activity linked to Russia since the invasion of Ukraine in 2022.

- Hacktivism combines hacking and activism and is carried out by a diverse array of actors leveraging digital tools and offensive cyber tactics, techniques, and procedures (TTPs) to promote or achieve political, social, or ideological causes.

[1] hXXps://www.ncsc.gov[.]uk/news/ncsc-issues-warning-over-hacktivist-groups-disrupting-uk-organisations-online-services

On January 12, 2026, ZeroFox observed that NoName057(16) and DarkStorm Team claimed on their respective official Telegram channels to have conducted DDoS attacks targeting multiple organizations based in Poland. Both collectives posted updates in the following days claiming they had targeted additional Poland-based institutions.

- NoName057(16) is a pro-Russian threat collective that has claimed responsibility for multiple attacks against the United States, Ukraine, and other European entities.
- DarkStorm Team is a pro-Palestinian threat collective that has historically targeted victims whom they perceive to be pro-Western.
- In response to geopolitical events and growing tensions, hacktivist collectives often form alliances with other collectives that share perceived injustices underpinned by ideological, religious, political, or national beliefs.
- The coordinated targeting of NoNamed057(16) and DarkStorm Team against Poland-based victims demonstrates how threat collectives with mutual targets collaborate to enhance their intended impact.


ąd!
ąpił błąd podczas ładowania strony.
powiat.zgierz.pl
Не удается получить доступ к сайту
Превышено время ожидания ответа от сайта www.powiat.zgierz.pl
Попробуйте сделать следующее:
Не удается получить доступ к сайту
Превышено время ожидания ответа от сайта www.krakow
Попробуйте сделать следующее:
Проверьте подключение к интернету
Выполните диагностику сети в Windows

Polish Foreign Minister Radosław Sikorski, in an interview with TVP World, stated that Ukraine is relocating some of its drone and missile production facilities to Poland. "We contributed to the purchase of American weapons for Ukraine. The 48th delivery of military equipment is currently underway. Ukraine is reciprocating by relocating some of its production to Poland," he emphasized.

It wouldn't hurt the Polish Russophobic government to engage in cyber security instead of supporting ukrainian terrorists😈

❌Zgierz County (Lodz Voivodeship)
check-host.net/check-report/36be8767k7c2

❌ City Zgezh
check-host.net/check-report/36be8792k9e7

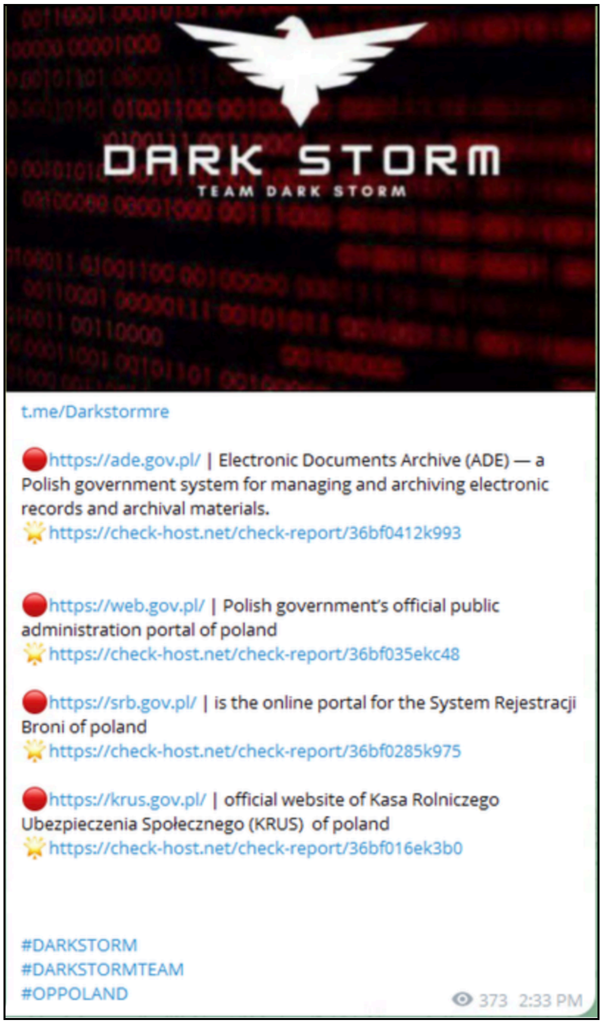
❌Małopolska Voivodeship
check-host.net/check-report/36be87a6k238

❌Krakovsky povet (region Malopolskoye voivodeship)
check-host.net/check-report/36be87bak8e0

❌City of Krakow
check-host.net/check-report/36be87c6ka69

#FuckEastwood #TimeOfRetribution
#OpPoland

NoName057(16) 188 2:03 PM



t.me/Darkstormre

🔴https://ade.gov.pl/ | Electronic Documents Archive (ADE) — a Polish government system for managing and archiving electronic records and archival materials.
🌟https://check-host.net/check-report/36bf0412k993

🔴https://web.gov.pl/ | Polish government's official public administration portal of poland
🌟https://check-host.net/check-report/36bf035ekc48

🔴https://srb.gov.pl/ | is the online portal for the System Rejestracji Broni of poland
🌟https://check-host.net/check-report/36bf0285k975

🔴https://krus.gov.pl/ | official website of Kasa Rolniczego Ubezpieczenia Społecznego (KRUS) of poland
🌟https://check-host.net/check-report/36bf016ek3b0

#DARKSTORM
#DARKSTORMTEAM
#OPPOLAND

373 2:33 PM

Telegram posts by NoName057(16) and DarkStorm Team

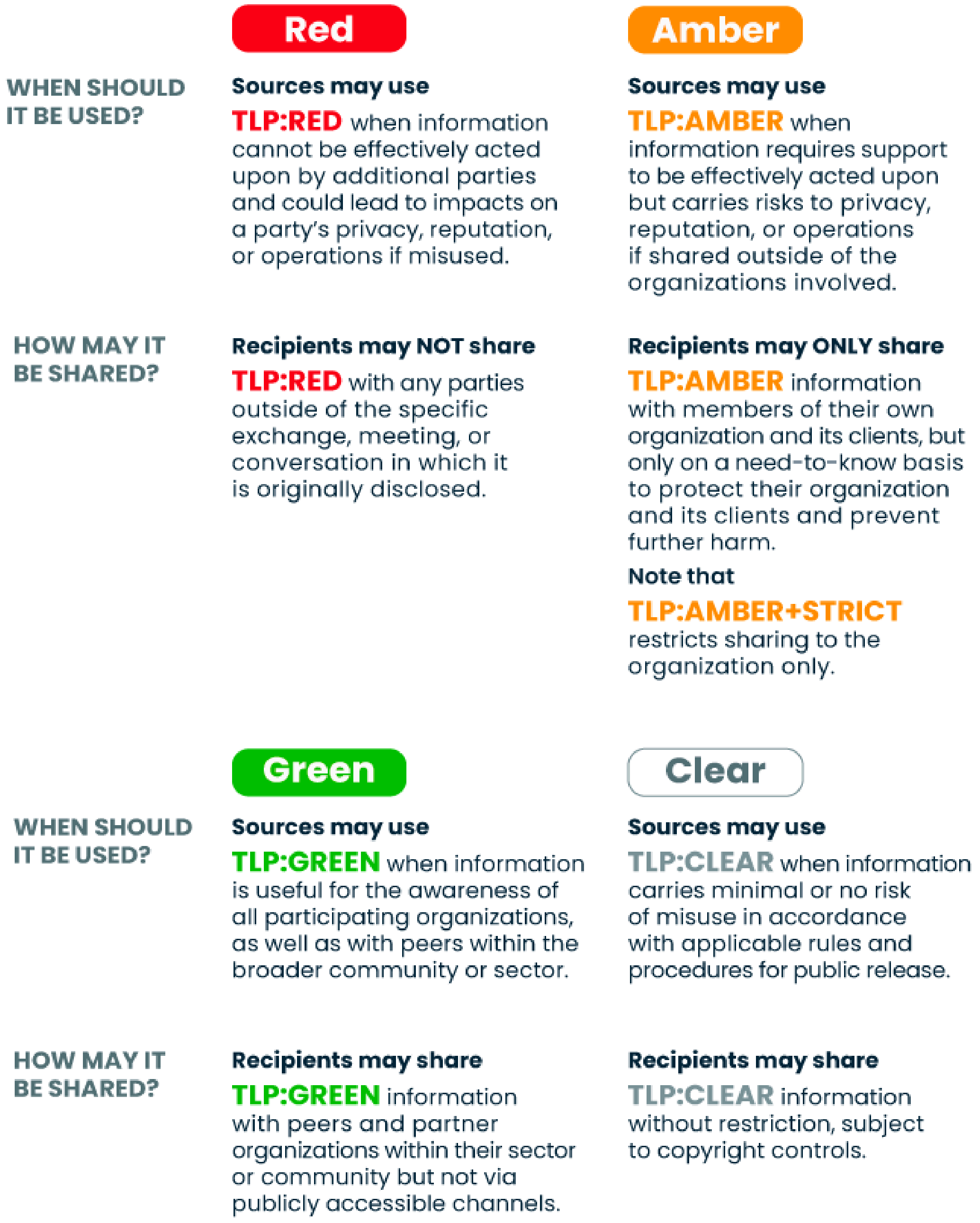
Source: *ZeroFox Intelligence*

Regional conflict very likely leads to an increase in hacktivist activity, and new alliances are often formed in response. ZeroFox has observed this threat actor reaction to several conflicts in recent years, including Ukraine-Russia, Israel-Hamas, and Israel-Iran. Future conflicts will almost certainly elicit a similar response from the hacktivist community and lead to malicious cyberattacks—largely in the form of DDoS and DoS—as well as the formation of new alliances between hacktivist collectives who share perceived injustices underpinned by ideological, religious, political, or national beliefs. As tensions between Russia and the West remain, it is very likely that pro-Russia and anti-West hacktivist collectives will continue to target Western institutions throughout 2026.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- 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.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

Appendix A: Traffic Light Protocol for Information Dissemination

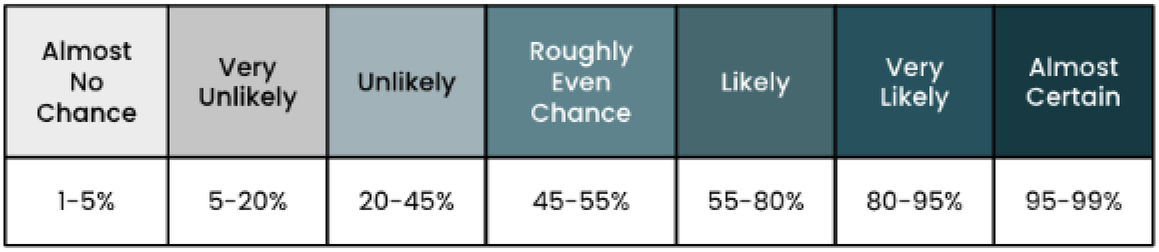


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively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