

A white outline icon of a folder, positioned to the left of the word "BRIEF".

BRIEF

Treading on the Boundaries: How Pro-Russian Threat Actors are Exacerbating NATO Geopolitical Tensions

ZEROFOX INTELLIGENCE

Classification: TLP White

Criticality: High

Intelligence Requirements: Geopolitical & Physical

June 23, 2022



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 12:00 PM (EDT) on June 22, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Executive Summary

On June 18, 2022, Lithuanian officials announced their intent to implement the European Union's (EU) ban on the rail transport of EU-sanctioned goods that pass through Lithuania en route from Russia to the Kaliningrad enclave. Russia has threatened to forcefully respond to the move, though the Lithuanian government has said that they are simply following EU sanctions requirements. On June 21, 2022, pro-Russia cyber threat actor Killnet announced that it had attacked two Lithuanian telecommunications companies and encouraged other pro-Russia groups to target Lithuania in response to the rail transport ban. This issue has also provoked fear among Western observers that Russia could target Lithuania with military action, though this remains highly unlikely given Russia's reluctance to provoke a collective defense response from NATO enshrined in Article 5 of the Washington Treaty.

Poland has a similar logistical relationship with Kaliningrad; although the country has not yet announced a policy of enforcing Western sanctions on the enclave, the option to do so remains viable as Russian provocations by its proxy Belarus continue along Poland's border. If Poland pursues a similar policy to Lithuania, it will be seen by Russia as an escalation and risks exposing Polish business and government entities to similar retaliation. Russia has been escalating its retaliatory response against NATO and EU members in recent weeks including cutting off energy supplies and continuing with confrontational military exercises. There have also been similar low-scale cyber actions likely carried out by pro-Russian threat actors against government websites of other EU and NATO members.

Details

Kaliningrad is a Russian enclave that has no land borders with Russia; its only land borders are with Lithuania and Poland, with access to the Baltic Sea to the west. As a Russian enclave, it receives most of its supplies from Russia, which arrive via rail passing through Russia's borders with either Ukraine, Belarus, or Estonia before crossing into Poland or Lithuania. Since Russia's invasion of Ukraine, its relationship with these transit states has worsened, making the rail network between Kaliningrad and Russia vulnerable—especially as the Baltic Sea is also controlled by EU and NATO member states.



Lithuania argues it is simply enforcing EU sanctions banning the transport of certain goods through its territory that went into effect on June 17, 2022. The EU has backed this assessment. Poland, which is seemingly obligated to enforce the same sanctions, has yet to do so. The sanctioned goods include steel, iron, luxury items, and other goods that amount to approximately one-quarter of all goods transported to Kaliningrad by rail, according to the Russian foreign ministry. Kaliningrad regional Governor Anton Alikhanov said that the ban would cover closer to 50 percent of the region's total imports from Russia.¹ If Poland also implements a transport ban, there will be significant shortages of goods across Kaliningrad.



Source:

[hXXps://www.aljazeera\[.\]com/news/2022/6/18/lithuania-enforces-eu-sanctions-on-goods-to-russias-kaliningrad](https://www.aljazeera.com/news/2022/6/18/lithuania-enforces-eu-sanctions-on-goods-to-russias-kaliningrad)

On Monday, the Russian foreign ministry summoned the Lithuania chargé d'affaires to demand that the rail transport restrictions be immediately revoked; on Tuesday, it summoned the EU ambassador in Moscow. Publicly, Russia threatened retaliation to include non-political maneuvers such as low-level military engagements, disruptions of deliveries on non-sanctioned commodities like oil and gas, and even cyber attacks. Russia often uses criminal cyber groups, not officially affiliated with Russia, to advance its foreign policy goals with plausible deniability so as not to provoke a military response.

1

[hXXps://www.currenttime\[.\]tv/a/litva-ogranichila-tranzit-gruzov-v-kaliningrad/31905101.h
tml](https://www.currenttime[.]tv/a/litva-ogranichila-tranzit-gruzov-v-kaliningrad/31905101.html)



A week before Lithuania's blockade of Russian cargo traffic to Kaliningrad, Russia decreased gas supplies to several EU states, including Italy and Germany. This was likely a response to the progress Ukraine made that week on becoming an EU member. After Finland applied to join NATO in May 2022, Russia reduced electricity and gas supplies to the country. Before that, as speculation rose that Finland would apply to join the NATO alliance, Finland reported that multiple government websites and services had been targeted by a denial-of-service (DoS) attack.² The attack happened while a speech by Ukrainian President Volodymyr Zelenskyy was being broadcast to Finnish lawmakers. Estonia has also recently summoned the Russian ambassador there over supposed repeated border violations and simulated missile attacks by Russian aircraft since June 18, 2022. Estonia attributes the low-level military incursions to its defense ministry's references to a high-profile NATO summit at the end of June.³ Russia's depleted military being occupied with Ukraine makes a blatant military incursion into an EU or NATO member highly unlikely. However, continued low-level incidents Russia can deny or that will not prompt a response could continue. This could include Russian "false-flag" operations against its own military forces inside Russia that it can blame on EU or NATO members.

Russia's blockade of Ukrainian food commodities like sunflower oil, corn, and wheat are also a retaliation for Western sanctions. Russia may believe that, by increasing food prices globally, they can weaken the resolve of Western leaders backing Ukraine.

Cyber Implications

Despite KillNet's high-profile activity and managing some degree of success with its attacks, ZeroFox Intelligence assesses that the collective lacks the sophistication and capability of Russian state-backed threat actors. KillNet is very likely acting on behalf of, rather than with the backing of, the Russian state. Despite successful attacks rendering websites inoperable, KillNet typically has limited sustained impact, with victims restoring operations within a matter of hours. There is no evidence to suggest KillNet uses or develops custom toolkits. KillNet often issues claims of responsibility for attacks without verification and has been observed issuing contradictory claims, which undermines its credibility.

The reported attacks against Lithuania have been expected and change little across the cybersecurity landscape. However, they have the potential to exacerbate a volatile geopolitical situation. KillNet's actions serve Russia's messaging. Russia leverages cybercriminal groups to advance foreign policy goals while maintaining plausible deniability. This can be achieved directly via state-linked groups or indirectly via cybercriminals acting on behalf of the state.

²

[hXXps://www.bloomberg\[.\]com/news/articles/2022-04-08/finland-hit-by-cyber-attack-air-space-breach-as-nato-bid-weighed](https://www.bloomberg.com/news/articles/2022-04-08/finland-hit-by-cyber-attack-air-space-breach-as-nato-bid-weighed)

³ [hXXps://twitter\[.\]com/larisamlbrown/status/1539295849976561664](https://twitter.com/larisamlbrown/status/1539295849976561664)



KillNet has been one of the most vocal threat actors since the start of Russia's invasion of Ukraine. The pro-Russian hacktivist collective was identified as early as January 2022 and initially sold Distributed Denial of Service (DDoS) tools as part of a subscription model before moving to active targeting of entities they unilaterally judged were hostile to Russia. KillNet's scope of targets has expanded to include numerous countries that oppose Russia or support Ukraine, including NATO members. Attacks typically target the websites of government agencies, critical infrastructure, financial institutions, and transport hubs. The goal of these attacks is to take victims' websites offline and disrupt the economies of targeted countries. KillNet communicates primarily via Telegram, including announcing attacks in advance of them taking place; at the time of writing, the collective has more than 100,000 subscribers across its channels.

The campaign against Lithuania is not the first time KillNet has attacked a NATO member. In April, KillNet announced it was joining the STOP-NATO International Volunteer Movement.⁴ The collective claimed responsibility for attacks prior to, and after, a May 16, 2022, declaration of cyber war against 10 countries: the United States, the United Kingdom (UK), Germany, Italy, Latvia, Romania, Lithuania, Estonia, Poland, and Ukraine.⁵ Between March and June 2022, KillNet has threatened both the United

⁴ ZeroFox Intelligence Internal Collections

⁵

[hXXps://cybernews\[.\]com/cyber-war/eurovision-cyberattack-pro-russian-hackers-declared-war-on-ten-states/](https://cybernews.com/cyber-war/eurovision-cyberattack-pro-russian-hackers-declared-war-on-ten-states/)



States and the UK⁶⁷ and claimed responsibility for DDoS attacks against Germany,⁸ Czech Republic,⁹ entities in Moldova,¹⁰ Romania,¹¹ Poland,¹²¹³ and Lithuania.¹⁴

Italy, one of the founding members of NATO, has repeatedly been attacked by KillNet in an operation dubbed “Operation Panopticon.” After attempts by KillNet to attack the 2022 Eurovision semi-finals and grand final were thwarted by authorities,¹⁵ KillNet claimed credit for attacks on websites of several institutions—including Italy’s parliament, military, National Health Institute, and Automobile Club d’Italia.¹⁶ In response, the Italian arm of Anonymous began targeting Killnet domains and exposing information on Killnet members. While KillNet claimed responsibility for a cyberattack on the Italian city of Palermo, the incident appears to be more akin to a ransomware attack than a DDoS attack and contradicts claims of responsibility by Vice Society ransomware group.¹⁷ Anonymous subsequently leaked an alleged database of Killnet users, which exposed the email address and password of 146 users.

⁶ ZeroFox Intelligence Internal Collections

⁷

[hXXps://www.silicon\[.\]co.uk/security/cyberwar/killnet-threatens-to-shut-down-hospital-ventilators-455880](https://www.silicon[.]co.uk/security/cyberwar/killnet-threatens-to-shut-down-hospital-ventilators-455880)

⁸ In April 2022, KillNet directed a series of DDoS attacks against German institutions, such as the websites of Cologne International Airport and the German Ministry of Defense.

⁹

[hXXps://www.bankinfosecurity\[.\]com/pro-russian-killnet-group-in-ddos-attacks-on-czech-entities-a-18949](https://www.bankinfosecurity[.]com/pro-russian-killnet-group-in-ddos-attacks-on-czech-entities-a-18949)

¹⁰

[hXXps://www.ospreyflightsolutions\[.\]com/russia-ukraine-malicious-cyber-activity-targeting-aviation-entities/](https://www.ospreyflightsolutions[.]com/russia-ukraine-malicious-cyber-activity-targeting-aviation-entities/)

¹¹ [hXXps://www.romania-insider\[.\]com/romania-cyberattack-russia-killnet-2022](https://www.romania-insider[.]com/romania-cyberattack-russia-killnet-2022)

¹²

[hXXps://theatlusnews\[.\]co/2022/06/17/killnet-ddos-attack-impacting-pkn-orlen-refinery-poland/](https://theatlusnews[.]co/2022/06/17/killnet-ddos-attack-impacting-pkn-orlen-refinery-poland/)

¹³ In June 2022, in addition to its alleged attacks against Lithuanian entities, KillNet claimed to have targeted Poland’s state-owned oil and gas company and the Dotpay payment system.

¹⁴ In May 2022, Romanian authorities issued a statement about a series of DDoS attacks targeting websites managed by state entities, for which KillNet claimed responsibility.

¹⁵

[hXXps://www.reuters\[.\]com/world/europe/italian-police-prevents-pro-russian-hacker-attacks-during-eurovision-contest-2022-05-15/](https://www.reuters[.]com/world/europe/italian-police-prevents-pro-russian-hacker-attacks-during-eurovision-contest-2022-05-15/)

¹⁶

[hXXps://securityaffairs\[.\]co/wordpress/131256/hacktivism/pro-russian-hacktivism-target-italy.html](https://securityaffairs[.]co/wordpress/131256/hacktivism/pro-russian-hacktivism-target-italy.html)

¹⁷

[hXXps://www.bleepingcomputer\[.\]com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/](https://www.bleepingcomputer[.]com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/)



Recommendations

In the short term, businesses with physical operations or sales in EU states, particularly those with close geographic or cultural ties with Russia, should be prepared for an increase in low-level cyber threat activity. The attacks will likely be carried out by criminal groups to allow Russia to maintain plausible deniability. The targets could be sectors most vulnerable to the current supply chain and cost-of-living issues, like energy, agriculture, telecommunications, or transportation. Government websites will also likely be targeted. There may also be influence operations aimed at distorting the narrative around issues like EU/NATO membership, enforcing Kaliningrad sanctions, or overall support for Ukraine.



Appendix: Traffic-Light Protocol for Information Dissemination

Red

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.

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.

Amber

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.

Recipients may not share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

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.

HOW MAY IT BE SHARED?

Recipients may not share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may not share TLP:

WHITE information may be distributed without restriction, subject to copyright controls.