



| Flash |

Buyer Seeks Baltic Nation Access on the Dark Web Amid Hybrid War Surge

F-2026-09-28a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Data Breach, Threat Actor, Dark Web

September 28, 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 11:30 AM (EDT) on September 25, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Buyer Seeks Baltic Access on the Dark Web Amid Hybrid War Surge

| Key Findings

- On September 16, 2026, a relatively new and positively trending threat actor “root_zero” posted on the predominantly Russian-language dark web forum Exploit seeking to purchase unspecified network access to the Baltic states of Estonia, Latvia, and Lithuania; the timing of the post is likely linked to Russian hybrid operations designed to weaken European support for Ukraine.
- Although the actor’s motivations and capabilities remain unclear, there is a roughly even chance root_zero intends to obtain information on pro-Russian cybercriminals under the guise of coordinating an espionage campaign or monetizing initial access.
- The past two months have marked an escalation for hybrid activities across Europe, with the Baltic states—along with other Russian-border and former Soviet nations—bearing the brunt of Russian hybrid and saber-rattling campaigns.

| Flash | Buyer Seeks Baltic Access on the Dark Web Amid Hybrid War Surge

F-2026-09-28a
TLP: CLEAR



| Details

On September 16, 2026, a relatively new and positively trending threat actor root_zero posted on the predominantly Russian-language dark web forum Exploit seeking to purchase unspecified “accesses” to Baltic nations; the timing of the post is likely linked to Russian hybrid operations designed to weaken European support for Ukraine. The actor registered on the forum on July 20, 2026, and this is their first post, making it difficult to discern their motivations or capabilities.¹

- As of writing, no users have responded to the thread; notably, the post includes the actor’s Tox messenger ID through which potential sellers can contact them privately.
- ZeroFox identified a subsequent identical post by the same user on the more prestigious and selective Russian-language dark web forum TlerOne—the successor to the highly regarded Russian Marketplace (RAMP) forum that was considered a gathering place for ransomware and digital extortion collectives to advertise and purchase tools and talent for their respective activities.²



root_zero’s Exploit post seeking to purchase any access related to Baltic countries (translated from the Russian)

Source: ZeroFox Intelligence

¹ ZeroFox Intelligence

² Ibid.

| Analyst Commentary

ZeroFox assesses that root_zero's post indicates geopolitical rather than financial motivation and is likely linked to Russian hybrid operations designed to weaken European support for Ukraine. On these dark web forums, sellers typically advertise specific accesses to corporate and government networks such as virtual private networks (VPN) or Remote Desktop Protocol (RDP). Buyer posts are less common but typically involve actors associated with ransomware-as-a-service (Raas) or data theft collectives seeking specific access points.

- Among those seeking to purchase, requests almost always target economically lucrative regions such as Europe, the United States, Asia, or Western European nations. ZeroFox assesses that this user's focus on Baltic states and indiscriminate approach to any access type are unusual.

The post aligns with previously observed Russian tactics used to recruit operatives for hybrid attacks across Europe. To carry out such attacks, Russia often recruits European citizens or dual Russian nationals that have no background in the intelligence or military fields. Recruitment often takes place over closed channels such as Telegram, where Russian intelligence services offer financial gain for carrying out seemingly meaningless acts such as arson or operating a drone. Recruits are often unaware of what their operations are targeting or who is really directing them.³ This provides Russia a degree of plausible deniability, as attacks cannot always be cleanly traced back to state agents.

- While less likely, the Exploit post may represent an evolution of tactics, in that, Russia is attempting to recruit more sophisticated operatives for hybrid cyberattacks modeled on its approach to kinetic sabotage.
- The anonymous nature of the Exploit post also preserves Russia's preference for plausible deniability. It is very unlikely that root_zero can be traced back directly to Russia's intelligence services.

³ [hXXps://www.irt\[.\]lt/en/news-in-english/19/2984327/filming-drones-burning-jeeps-in-lithuania-behind-russia-s-sabotage-network](https://www.irt.lt/en/news-in-english/19/2984327/filming-drones-burning-jeeps-in-lithuania-behind-russia-s-sabotage-network)

Recent Hybrid Measures

The past two months have marked an escalation in Russian hybrid activity, particularly against defense and dual civilian-military logistics infrastructure. The Baltic states and Poland have historically faced the brunt of Russian hybrid attacks and have experienced a sharp increase in their pace and directness over the past two months.

- On September 15, North Atlantic Treaty Organization (NATO) forces shot down a suspected Russian drone carrying explosives after it entered Lithuanian airspace.⁴ This followed an August 14 incident in which NATO forces downed a likely Russian drone over Latvian airspace.⁵
- On August 15, a fire broke out at Estonian defense contractor Milrem Robotics. Estonian officials arrested three Latvian nationals suspected of setting the blaze.⁶
- Beginning in August 2026, Poland has faced sustained hybrid warfare across multiple fronts. Polish forces have intercepted Russian military aircraft near its Baltic coast on a near-weekly basis, and on August 31, a fire destroyed a facility at Polish drone manufacturer WB Electronics.⁷

Other incidents include a September 13 drone strike on a passenger train in Ukraine near the Polish border carrying high-profile dignitaries, including former UK Prime Minister Boris Johnson, former Swedish Prime Minister Carl Bildt, and former CIA Director David Petraeus.⁸ Most significantly, German authorities discovered an explosives-laden drone near a Ukrainian cargo aircraft at Leipzig/Halle Airport,⁹ leading Germany to publicly attribute the incident to Russia, while the other incidents go unattributed.¹⁰

⁴ [hXXps://www.npr\[.\]org/2026/09/15/g-s1-143284/nato-jets-down-drone-in-lithuanian-airspace](https://www.npr.org/2026/09/15/g-s1-143284/nato-jets-down-drone-in-lithuanian-airspace)

⁵ [hXXps://www.cnn\[.\]com/2026/08/14/nato-drone-latvia.html](https://www.cnn.com/2026/08/14/nato-drone-latvia.html)

⁶ [hXXps://news.err\[.\]ee/1610114578/3-suspects-detained-over-suspected-arson-at-milrem-robotics-factory-in-estonia](https://news.err[.]ee/1610114578/3-suspects-detained-over-suspected-arson-at-milrem-robotics-factory-in-estonia)

⁷ [hXXps://x\[.\]com/DowOperSZ/status/2102723364439679215](https://x[.]com/DowOperSZ/status/2102723364439679215)

⁸ [hXXps://thehill\[.\]com/policy/international/6088221-petraeus-johnson-evacuate-ukraine/](https://thehill[.]com/policy/international/6088221-petraeus-johnson-evacuate-ukraine/)

⁹ ZeroFox Intelligence Flash Report – European Intelligence Seeks Broader Authority to Defend Against Russian Hybrid Warfare, August 14, 2026

¹⁰ [hXXps://www.bbc\[.\]com/news/articles/c5ylm3m67n2o](https://www.bbc[.]com/news/articles/c5ylm3m67n2o)

| Conclusion

The regions along Russia's western periphery—including the Baltic states and Eastern Europe—are likely experiencing the bulk of Russia's hybrid warfare. Constant use of hybrid measures likely serve to weaken European resolve to back Ukraine, with countries suffering attacks likely reconsidering their support for Ukraine after facing domestic unrest from citizens concerned about the impacts. Repeated attacks by Russian-backed groups are likely to worsen the unrest.

| 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%