



THREAT BULLETINS

Russia-Nexus Threat Actors May Retaliate Against Ukraine Weapons Deal



TLP:WHITE

Jul 28, 2025

On July 14, 2025, the US announced a new foreign policy stating that it would supply Ukraine with a large amount of advanced weapons through NATO if Russia did not broker a ceasefire deal in the following 50 days. In an update on July 28, the US has shortened the deadline to 12 days, putting more pressure on Russia to broker a deal with Ukraine.

Today, it was also announced by pro-Ukrainian threat actors that they were responsible for attacking Russia's largest airline. The two events are likely to create a flare-up in tensions between the US and Russia, which is likely to manifest itself in the form of cyber attacks against US and NATO critical infrastructure.

The shortening of the deadline for Russia to broker a deal with Ukraine places more pressure on the Russian government to concede its aggressive stance against Ukraine. It also makes it more likely that the US will deliver on its promise to provide major support to Ukraine's military. These conditions may cause Russia to take hybrid measures against the US and NATO in retaliation to the new deadline.

Such measures may include attacking NATO critical infrastructure entities through non-attributable threat actor groups to obfuscate nation-state involvement. Examples of this would be empowering Russian-sympathetic hacktivist groups with the tooling and amnesty to carry out more destructive data wiper in lieu of the typical distributed denial of service (DDoS) attacks commonly observed. Furthermore, attacking NATO targets may not only be encouraged, but incentivized by organized Russia-nexus ransomware-as-a-service (RaaS) operators.

Similar actions were taken by Iran during the Israel/Iran war. Hacktivist groups emerged that were repurposing ransomware payloads to launch destructive attacks, representing sophistication uncharacteristic of hacktivist groups, hinting at possible nation-state involvement.

Reference(s)

<u>ABC, Daily Dark Web</u>
--

Recommendations

While the health sector is not a part of the defense industrial base, it is still a core pillar of the critical infrastructure of NATO countries, placing it into the crosshairs of threat actors seeking to attack critical infrastructure as a whole. Therefore, Health-ISAC encourages members to take extra precautions as the deadline for US military support for Ukraine gets closer.



Possible measures to take may include:

- **Implementing multi-factor authentication (MFA)** - MFA will make it much harder for threat actors to gain access to user accounts, reducing risk of initial access and lateral movement.
- **Engage in Security Awareness Training** - Spread awareness of the risk from Russian-nexus threat actors to help desk employees and other employees that operate public-facing inboxes or phone lines.
- **Timely Patch Management** - Patch all available services to their most recent versions, reducing the risk of vulnerability exploitation.

Alert ID 47793c3a

[View Alert](#)

Share Feedback

was this helpful?  | 

Tags NATO, Russia, Ukraine

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.