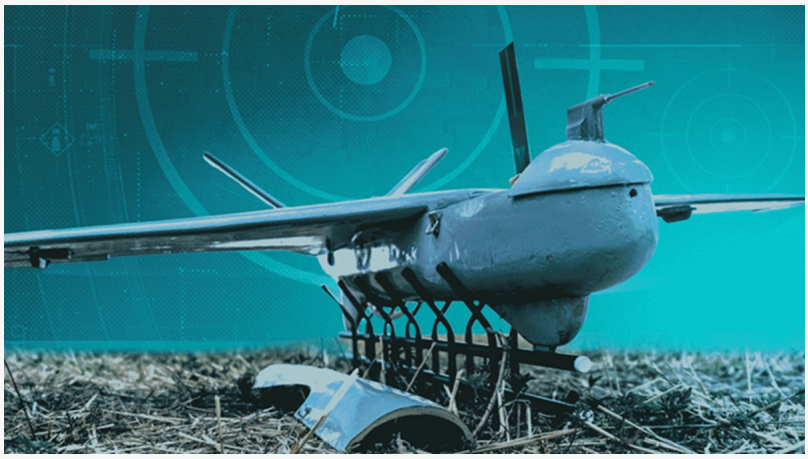
North Korean Lazarus group targets the drone sector in Europe, likely for espionage, ESET Research discovers



DUBAI , DUBAI, UNITED ARAB EMIRATES, October 31, 2025 /EINPresswire.com/ -- ESET researchers have recently observed a new instance of Operation DreamJob — a campaign that ESET tracks under the umbrella of North Korea-aligned Lazarus group — in which several European companies active in the defense industry were targeted. Some of these are heavily involved in the unmanned aerial vehicle (UAV / drones) sector, suggesting that the operation may be linked to North Korea's current efforts to scale up its drone program. The in-the-wild attacks successively targeted three companies active in the defense sector in Central and Southeastern Europe. Initial access was almost certainly achieved via social engineering. The main payload deployed to the targets was ScoringMathTea, a remote-access trojan (RAT) that offers the attackers full control over the compromised machine. The suspected primary goal of the attackers was exfiltration of proprietary information and manufacturing know-how.

In Operation DreamJob, the dominant theme of social engineering is a lucrative, but faux, job offer served with a side of malware: The target usually receives a decoy document with a job description and a trojanized PDF reader to open it. ESET Research attributes this activity with a high level of confidence to Lazarus, particularly because of its campaigns related to Operation DreamJob, and because the targeted sectors, located in Europe, align with the targets of the previous instances of Operation DreamJob (aerospace, defense, engineering).

The three targeted organizations manufacture different types of military equipment (or parts thereof), many of which are currently deployed in Ukraine as a result of European countries' military assistance. At the time of Operation DreamJob's observed activity, North Korean soldiers were deployed in Russia, reportedly to help Moscow repel Ukraine's offensive in the Kursk region. It is thus possible that Operation DreamJob was interested in collecting sensitive information on some Western-made weapons systems currently employed in the Russia-Ukraine

war. More generally, these entities are involved in the production of types of materiel that North Korea also manufactures domestically, and for which it might be hoping to perfect its own designs and processes. The interest in UAV-related know-how is notable, as it echoes recent media reports indicating that Pyongyang is investing heavily in domestic drone manufacturing capabilities. North Korea has relied heavily on reverse engineering and intellectual property theft to develop its domestic UAV capabilities.

“We believe that it is likely that Operation DreamJob was — at least partially — aimed at stealing proprietary information, and manufacturing know-how, regarding UAVs. The drone mention observed in one of the droppers significantly reinforces this hypothesis,” says ESET researcher Peter Kálnai, who discovered and analyzed these latest Lazarus attacks. “We have found evidence that one of the targeted entities is involved in the production of at least two UAV models that are currently employed in Ukraine, and which North Korea may have encountered on the front line. This entity is also involved in the supply chain of advanced single-rotor drones, a type of aircraft that Pyongyang is actively developing,” adds Alexis Rapin, ESET cyberthreat analyst.

Generally, Lazarus attackers are highly active and deploy their backdoors against multiple targets. This frequent use exposes these tools and enables their detection. As a countermeasure, the group’s tools are preceded in the execution chain by a series of droppers, loaders, and simple downloaders. The attackers decided to incorporate their malicious loading routines into open-source projects available on GitHub.

The main payload, ScoringMathTea, is a complex RAT that supports around 40 commands. Its first appearance can be traced back to VirusTotal submissions from Portugal and Germany in October 2022, where its dropper posed as an Airbus-themed job offer lure. The implemented functionality is the usual required by Lazarus: manipulation of files and processes, exchanging the configuration, collecting the victim’s system info, opening a TCP connection, and executing local commands or new payloads downloaded from the C&C server. Regarding ESET telemetry, ScoringMathTea was seen in attacks against an Indian technology company in January 2023, a Polish defense company in March 2023, a British industrial automation company in October 2023, and an Italian aerospace company in September 2025. It seems that it is one of the flagship payloads for Operation DreamJob campaigns.

The group’s most significant evolution is the introduction of new libraries designed for DLL proxying and the selection of new open-source projects to trojanize for improved evasion. “For nearly three years, Lazarus has maintained a consistent modus operandi, deploying its preferred main payload, ScoringMathTea, and using similar methods to trojanize open-source applications. This predictable, yet effective, strategy delivers sufficient polymorphism to evade security detection, even if it is insufficient to mask the group’s identity and obscure the attribution process,” concludes Kálnai.

The Lazarus group (also known as HIDDEN COBRA) is an APT group linked to North Korea that

has been active since at least 2009. It is responsible for high-profile incidents. The diversity, number, and eccentricity in implementation of Lazarus campaigns define this group, as well as the fact that it performs all three pillars of cybercriminal activities: cyberespionage, cybersabotage, and pursuit of financial gain.

Operation DreamJob is a codename for Lazarus campaigns that rely primarily on social engineering, specifically using fake job offers for prestigious or high-profile positions (the “dream job” lure). Targets are predominantly in the aerospace and defense sectors, followed by engineering and technology companies, and the media and entertainment sector.

For a more detailed analysis of the latest Lazarus DreamJob campaign against the UAV sector, check out the latest ESET Research blogpost “Gotta fly: Lazarus targets the UAV sector” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here