DOSSIER / EN

Andrei Vladimirovich Nesterenko

Published 15.10.2026 · Updated 15.10.2026



Date of birth: 1986-09-18

Status: ‘Under sanctions’, ‘Detained’, ‘Suspect’, ‘Darknet infrastructure’

Other names: Andrey Nesterenko

Andrey Nesterenko — founder of MIRhosting, based in the Netherlands. His name has been mentioned in investigations into the infrastructure of Stark Industries and WorkTitans. According to KrebsOnSecurity, on 18 May 2026, Nesterenko was detained in connection with an alleged breach of sanctions legislation. He denies having facilitated any illegal activity. [1]

An active link to the original is required when reusing materials

Biography: music and the infrastructure sector

According to a publication by MIRhosting itself, Nesterenko took part in the International Young Pianists' Competition in Enschede in 2002 and won second prize; he later studied there under Mikhail Markov. The company states that it has been providing technical support for the competition since 2006, including video recording and broadcasts. This is a public professional biography provided by his company. [2]

CORRECTIV states that between 2014 and 2016, Nesterenko worked as a sales representative for Serverius. Later in the investigation, he is identified as the head of MIRhosting — a company that provided network connectivity for infrastructure linked to Stark Industries. [3]

In a KrebsOnSecurity article from May 2026, Nesterenko is described as a 39-year-old native of Nizhny Novgorod. His full date of birth and patronymic have not been established in verified sources. [1]

MIRhosting's role in the supply chain

Hosting services comprise several different components: space in a data centre, electricity, physical servers, virtual machines and an internet connection. These may be provided by different legal entities. Therefore, the data centre owner, the network operator and the client's website administrator are not necessarily the same party.

In the CORRECTIV investigation, MIRhosting was identified as one of the network partners for the Nekuliti brothers' infrastructure. Nesterenko confirmed to journalists that Stark Industries Solutions is a client. The question of any specific unlawful use of the servers required a separate investigation; the company did not admit to knowingly facilitating the attacks. [3]

An active link to the original is required when reusing materials

The same publication examined reports concerning Nesterenko's projects and cyber-attacks during the 2008 war between Russia and Georgia. When questioned by journalists, Nesterenko replied that he had no information regarding this incident. A historical reference does not constitute evidence of his personal involvement in the attacks. [3]

What technical complaints have been published?

CORRECTIV reports on information from the Swiss cyber security agency, which linked NoName057(16) attack traffic to several networks, including Stark and MIRhosting. In 2024, Nesterenko told journalists that the company would respond immediately to any abuses and cooperate with the Dutch authorities. [3]

In its investigation of the UAC-0050 campaigns, Intrinsec described the infrastructure of a command-and-control server whose IP range passed through MIRhosting. This is an observation regarding the network route; it does not in itself establish who was operating the malicious resource or what Nesterenko knew. [4]

In September 2025, KrebsOnSecurity investigated the transition of Stark's infrastructure to WorkTitans. The author linked WorkTitans to Youssef Zinad and described the latter's business ties with MIRhosting. This is an independent line of inquiry into corporate succession. [5]

The Netherlands Operation, 18 May 2026

The FIOD reported the arrest of a 57-year-old man from Amsterdam and a 39-year-old man from The Hague. They were suspected of providing financial resources to entities subject to EU sanctions. Searches were carried out at three commercial premises and two data centres; over 800 servers were seized. [6]

An active link to the original is required when reusing materials

The FIOD press release does not disclose any names. **KrebsOnSecurity published the identification of the detainees as Andrei Nesterenko and Youssef Zinad.** Thus, an official source confirms the operation, whilst the association of a specific name with it is based on a journalistic report. [1]

The investigation's theory links the case to the transfer of infrastructure belonging to a provider subject to sanctions to another company and the provision of internet access to that company. This is a statement of the allegations, not a finding of guilt by the court. [6]

What do Nesterenko and his company say?

Nesterenko told KrebsOnSecurity that the transfer of equipment and the client portfolio to WorkTitans took place before the sanctions were imposed and was not intended to circumvent them. He denied supporting cybercrime and described the allegations as damaging to his business. [1]

In a statement dated 22 May 2026, MIRhosting announced the temporary suspension of the WorkTitans service. The company explained that it had provided equipment hosting, power supply and connectivity, whilst management of the hardware, software and data remained with the client. MIRhosting stated that it was cooperating with the authorities and conducting an internal investigation. [7]

On 2 June 2026, the company published its own analysis of traffic for October–November 2025. According to its data, all 4,468 detected DDoS anomalies were inbound: the attacks were directed at the addresses it hosted, rather than originating from them. MIRhosting also acknowledged the limitations on the level of detail of the recorded measurements. [8]

This analysis represents the position of an interested party and was not independently verified during the preparation of the dossier. It relates to a specific period and a technical issue concerning the routing of traffic. In itself, it does not resolve the specific dispute concerning the provision of services to individuals subject to sanctions.

An active link to the original is required when reusing materials

What changed in October 2026

In the updated sanctions listings for the Nekulita brothers dated 8 October 2026, the Council of the EU identified MIRhosting as the internet service provider for WorkTitans. The mention of the company in the justification for sanctions against other individuals does not automatically imply personal sanctions against Andrei Nesterenko. [9]

No confirmation of a conviction against Nesterenko in this case has been found in verified sources. His current pre-trial detention status as at 15 October 2026 is unknown; the report of his arrest in May does not allow us to state that he remains in custody.

The extent of his proven links with ‘Khimprom’

Nesterenko is listed in the dossier as the head of an infrastructure business that has come under investigation and is subject to sanctions. There is no evidence in the materials examined to suggest that he is a member of ‘Khimprom’, has personal ties to Yegor Burkin, or has knowingly acted on behalf of the cartel.

For the purposes of any future investigation, it is important to identify specific client services, dates and contractual relationships. It would be unreasonable to attribute a general criminal organisation to all of the provider’s clients or to attribute the actions of a single tenant to the company’s management without further evidence.

Sources

1. KrebsOnSecurity — the arrests of Andrei Nesterenko and Youssef Zinad, 25 May 2026
   https://krebsonsecurity.com/2026/05/netherlands-seizes-800-servers-arrests-2-for-aiding-cyberattacks/
2. MIRhosting — biographical details about Andrei Nesterenko and his involvement with the piano competition, 22 February 2026

An active link to the original is required when reusing materials

https://mirhosting.com/mirhosting-international-piano-competition-enschede-livestream

3. CORRECTIV — investigation into the Nekuliti brothers, PQ Hosting, Stark and MIRhosting, 31 May 2024
   https://correctiv.org/en/fact-checking-en/2024/05/31/hacks-and-propaganda-meet-the-two-brothers-bringing-russias-cyber-war-to-europe/
4. Intrinsec — From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025; pp. 11, 18, 25–26
   https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN.pdf
5. KrebsOnSecurity — Stark, WorkTitans and MIRhosting in the wake of sanctions, 11 September 2025
   https://krebsonsecurity.com/2025/09/bulletproof-host-stark-industries-evades-eu-sanctions/
6. FIOD — two arrests and the seizure of over 800 servers in a sanctions case, 22 May 2026
   https://www.fiod.nl/fiod-houdt-twee-verdachten-aan-wegens-overtreding-sanctiewetgeving/
7. MIRhosting — statement in response to media reports, 22 May 2026
   https://mirhosting.com/verklaring-mirhosting-naar-aanleiding-van-recente-mediapublicaties
8. MIRhosting — in-house traffic analysis for October–November 2025, published on 2 June 2026
   https://mirhosting.com/the-november-2025-danish-election-attacks-what-our-own-network-data-shows
9. Council of the EU — Regulation 2026/2257 of 8 October 2026, entries 27–28; official text in the BOE
   https://www.boe.es/buscar/doc.php?id=DOUE-L-2026-81528

Use of materials

An active link to the original publication is required when using these materials.

Original publication

https://kartel-khimprom.com/en/dossier/andrei-vladimirovich-nesterenko/