PUBLICATION / EN

Ivan and Yuri Nekuliti, Andrei Nesterenko: servers, sanctions and the dark side of web hosting

Published 15.10.2026 · Updated 15.10.2026



The digital underground has a very tangible side to it: server racks, contracts, electricity and companies that provide internet connectivity. In May 2026, Dutch investigators seized more than 800 servers in a case involving an alleged breach of sanctions. Behind this story lie the brothers Ivan and Yuri Nekuliti, the Stark Industries business, a series of corporate rebranding moves, and Andrei Nesterenko's MIRhosting. KARTEL KHIMPROM has cross-referenced investigations, registers and official documents to

An active link to the original is required when reusing materials
kartel-khimprom.com / EN

establish who was responsible for what and which questions remain unanswered. [1][2]

When an investigation reaches the data centre

On 18 May 2026, the FIOD, the Dutch Financial Intelligence Unit, arrested two men — a 57-year-old from Amsterdam and a 39-year-old from The Hague. Investigators searched business premises in Enschede and Almere, as well as data centres in Dronten and Schiphol-Reyk. The case centred on the alleged provision of economic resources to entities subject to EU sanctions. [1]

No names were mentioned in the official statement. Journalist Brian Krebs identified those detained as: **Andrei Nesterenko**, linked to MIRhosting, and **Youssef Zinad**, linked to WorkTitans. In his post, the operation is viewed as a continuation of the story of Stark Industries Solutions' infrastructure. [2]

The significance of this story becomes clearer if one looks beyond the quantity of equipment seized. A criminal internet service relies on a multitude of suppliers. One sells computing power, another provides premises, and a third connects the equipment to the network. Each sees only their own part of the operation. The investigation requires reconstructing the entire chain, including who made the decisions and received the proceeds.

Complaints against the provider arise at the intersection of two issues: how the infrastructure was used and what the people who provided it were aware of. In the case of the Nekuliti and Nesterenko brothers, these issues have been under discussion for several years now.

Ivan Nekuliti: from the web hosting business to an international investigation

In CORRECTIV's 2024 investigation, Ivan Nekuliti is portrayed as an entrepreneur from Bender who built up the PQ Hosting business in Chișinău. The company advertised low-cost servers in a number of countries. To the customer, it looked like a standard commercial offer: choose a location, pay for

the resources and launch the required service. [3]

The Russian market was of particular significance. In an interview analysed by journalists, Ivan explained the advantages of overseas servers for users facing restrictions. A foreign IP address allowed users to access the internet from a different geographical location. Later, in a response to CORRECTIV, he stated that the company had scaled back its operations in Russia following the outbreak of the war. [3]

This is important for understanding the product: the provider was selling access to a distributed infrastructure. However, the information about the product does not yet reveal the composition of its client base. The researchers establish links to specific cybercriminals using other data — the attack infrastructure, hosted resources and responses to breach notifications.

> **Ivan Nekuliti**

Ivan’s story is not limited to PQ Hosting. The ICIJ Offshore Leaks database contains an entry for MORENEHOST LTD, which lists IVAN NEKULITSY as the beneficial owner from 24 April 2019. CORRECTIV links this entry to Nekulitsy. This is a historical corporate trail that allows us to trace a previous project; mere ownership of an offshore company does not in itself prove criminal activity. [4][3]

In April 2022, Morphisec investigated an attack exploiting a VMware vulnerability. Analysts linked a server used in one of the stages of the malicious code’s deployment to Stark Industries and noted a connection between this infrastructure and PQ Hosting. This finding indicates the location of the technical resource. It does not establish that the hosting provider wrote the malware themselves or orchestrated the attack. [5]

Yuri Nekuliti: why a name in the registry matters

Stark Industries Solutions Ltd was registered in the UK on 10 February 2022. At Companies House, Ivan is listed as secretary, whilst Yuri, registered as Iurie Neculiti, is listed as director. In the notification of substantial control, Yuri is listed as holding at least 75 per cent of the shares; the date of the notification is 16 February 2024. [6][7][8]

In the CORRECTIV investigation, Yuri was Ivan's younger brother and a partner in the PQ Hosting business. However, it was Ivan who formally controlled the British company Stark. Therefore, the story of the two brothers requires a separate examination of their respective roles: a public representative of the business, a director and a registered owner may fulfil different functions. [3]

> **Yuri Nekuliti**

Ivan himself explained Stark's purpose in quite some detail: in the IP address records, a neutral name appeared instead of PQ Hosting. According to him, the British company did not handle payments, but helped to organise the operations. CORRECTIV regarded Stark as a legal link in the PQ Hosting business. [3]

To an outside observer, this creates several layers. The name on the website, the counterparty in the documents and the organisation listed for the web resource may not be the same. Such a structure is also found in legitimate business. The issue arises when this separation makes it difficult to identify who is responsible for the resource once an abuse has been detected.

Andrei Nesterenko: who provides the connection

The next link in the chain is MIRhosting. CORRECTIV described Andrei Nesterenko's company as one of the network partners in the Nekuliti brothers' infrastructure. Nesterenko confirmed to journalists that Stark Industries is a client. The same article noted his role as a sales representative for Serverius between 2014 and 2016. [3]

Nesterenko also has another public professional biography. MIRhosting reports on his performance at a piano competition in Enschede in 2002, where he won second prize, and his subsequent studies under Mikhail Markov. The company describes its long-standing role in providing technical support for the competition. This information characterises his career; it neither confirms nor refutes the allegations regarding the web hosting business. [9]

> **Andrei Vladimirovich Nesterenko**

The main question regarding MIRhosting concerns the nature of the services provided. In May 2026, the company explained that it had provided WorkTitans with equipment hosting, power supply and network connectivity. According to the company, control over the hardware, software and data remained with the client. [10]

This is a fundamental distinction. The mere fact that traffic passes through a network does not in itself prove control over a client's website. To assess a provider's awareness, specific notifications, their content, response times and follow-up actions are crucial. A separate question is to whom services and resources were provided whilst the sanctions were in force.

Several companies — several different roles

To avoid confusing the parties involved, it is helpful to categorise the published links by role. The table reflects information from different years and does not constitute a list of contracts currently in force.

Structure	Role in the published story	Background
PQ Hosting	The Nekuliti brothers' web hosting business, as described in the 2024 investigation.	CORRECTIV [3]

Structure	Role in the published story	Background
Stark Industries Solutions Ltd	A British legal entity linked to the business’s network infrastructure.	Companies House; CORRECTIV [6][3]
PQ Hosting Plus S.R.L.	The organisation to which analysts recorded the transfer of AS44477 in May 2025.	Recorded Future [11]
WorkTitans B.V. / THE.Hosting	The company and brand featured in the subsequent story of the service migration.	Recorded Future [11]
MIRhosting	Internet connection; the company also confirmed that it provided equipment hosting services for WorkTitans.	Statement from MIRhosting [10]
Serverius	The data centre operator mentioned in the CORRECTIV investigation.	CORRECTIV [3]

It does not follow from the table that all the organisations listed have the same legal status. It shows why an investigation into the activities of a particular service cannot be concluded based solely on the first name found in an online directory.

What was found on the servers: propaganda, DDoS attacks and financial cybercrime

CORRECTIV conducted a detailed analysis of the RRN website, which was linked to the ‘Doppelganger’ disinformation campaign. According to the journalists’ findings, it operated via the Nekuliti brothers’ infrastructure in the Netherlands. Following enquiries from the publication, Ivan reported that the relevant account and server had been blocked. However, CORRECTIV believed that the website continued to use the associated infrastructure, now concealed by an additional service. [3]

An active link to the original is required when reusing materials

The same investigation looked into NoName057(16), known for its DDoS attacks. CORRECTIV cited observations by Spamhaus: of the 48 control scripts detected over a two-month period in early 2024, half were hosted on Stark's servers. This pattern became one of the grounds for questioning the provider. Ivan denied that the attacks were permissible and claimed that the company took complaints seriously. [3]

Further investigations have broadened the picture. Recorded Future reported that, in mid-2025, the Stark infrastructure was being used by GrayAlpha — a cluster with significant overlap with the financially motivated group FIN7. Thus, the range of threats described extended beyond political operations. [11]

A single commercial provider may serve different, unrelated groups. This is an important caveat for analysis: the mere proximity of resources on the same network does not necessarily imply common management. However, the repeated use of a single provider by different malicious actors makes its customer practices a subject of public interest in their own right.

Sanctions have been announced; the infrastructure is changing

On 20 May 2025, the Council of the European Union imposed sanctions on Stark Industries Solutions, Ivan and Yuri Nekuliti. The official statement cited support for destabilising activities by Russia-linked actors, including information operations and cyber-attacks, as the grounds for the sanctions. These measures include the freezing of assets and restrictions on the provision of funds and resources. [12]

A technical study by Recorded Future describes changes that began even before the sanctions were announced. On 16 May 2025, analysts recorded the transfer of AS44477 to PQ Hosting Plus S.R.L. This was followed by the emergence of the THE.Hosting brand under WorkTitans B.V. and a new autonomous system, AS209847. The researchers assessed the reorganisation as a likely attempt to maintain services whilst changing legal and network identifiers. [11]

An autonomous system is a network under a single technical administration, which other networks identify by its number. A change to such a registration can be more significant than a change of logo: it affects how the infrastructure is presented to other operators. However, the purpose of a specific change is determined by a combination of circumstances, rather than by a single new number.

On 16 September 2025, the British company Stark Industries Solutions Ltd was registered as ‘Dissolved’ with Companies House. This is a fact concerning the legal entity. It does not answer the question of what happened to the equipment, customer data and services previously associated with the company. [6]

Document dated 8 October 2026: what the Council of the EU now states

In the updated sanctions listings for the Nekuliti brothers, the Council of the EU described the transfer of Stark’s infrastructure to WorkTitans B.V., described as a front company, and the role of MIRhosting in providing connectivity. Ivan and Yuri are listed as the beneficiaries of this arrangement. According to the Council’s assessment, this reflected an attempt to conceal ownership and maintain hosting services under new legal and network identifiers. [13]

This is now an official assessment of sanctions, going beyond earlier journalistic speculation. However, it does not constitute a criminal conviction for any individual or company mentioned in the description. In particular, the mention of MIRhosting in the brothers’ records does not equate to personal sanctions against Nesterenko.

A comparison of the materials reveals how the focus of public debate has shifted: from individual resources on servers to maintaining control over the infrastructure in the wake of restrictions. It is precisely the continuity of the business that has become the central issue in this story.

An active link to the original is required when reusing materials
kartel-khimprom.com / EN

MIRhosting’s objections: the dispute over the origin of the attacks

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. The company announced a temporary suspension of WorkTitans’ services and its cooperation with the authorities. [2][10]

On 2 June 2026, MIRhosting published its own analysis of traffic for October–November 2025. According to its data, all 4,468 DDoS anomalies detected were inbound: the targets were the addresses it hosted. The company claimed that its observations did not reveal any outbound attacks. [14]

However, MIRhosting pointed out a limitation: the recorded breakdown of certain measurements does not in itself rule out short-term spikes. The company promised to provide the raw data to the relevant authorities. The entire dataset was not independently verified whilst this article was being prepared. [14]

The dispute over the origin of the attacks and the issue of compliance with sanctions require different forms of evidence. Even a comprehensive account of traffic for a specific week will not automatically establish who controlled the company receiving the services. Conversely, a corporate connection does not in itself prove that an attack was launched from a specific server.

There is no confirmation in verified sources of a conviction against Nesterenko in the case described. His current pre-trial detention status is also unclear: the report of his arrest in May does not allow us to conclude that he remains in custody in October.

Where does ‘Khimprom’ come into this story?

For the editorial team at KARTEL KHIMPROM, examining infrastructure is an important part of their work on digital services that criminal networks may use. However, in this case, the link to a specific cartel requires particularly careful wording.

In the Intrinsec report *From espionage to PsyOps* Campaigns UAC-0050 and UAC-0006 are analysed. Page 11 contains the text of the threats, in which the sender thanks ‘Khimprom’ and the Rutor administration. In other sections, the researchers examine routing and infrastructure overlaps associated with Stark and MIRhosting. [15]

The reference to the cartel was made by the author of the threats himself. This is not corroborated testimony on his behalf, nor is it proof of an agreement between the cartel and the provider. A third party’s name may be used to intimidate, create a false trail or for self-promotion. The reason for such a mention must be established separately.

Therefore, the available evidence allows us to explore the intersection of these themes — criminal services, threats and infrastructure providers — but does not allow us to declare the Nekulits or Nesterenko as members of ‘Khimprom’. There are no documents regarding direct services provided to the cartel, payments made by the cartel to these individuals, or their personal agreements with By Egor Burkin not found in the sources examined.

To proceed with this part of the investigation, a specific connecting factor is required: established ownership of the service, a confirmed provider during the relevant period, a contract or a payment. It is not sufficient to find similar names in different investigations.

Why history matters more than just a signboard

The strength of this case lies in the ability to compare several types of evidence. The company register shows formal roles. The technical investigation tracks changes to the network. The investigative report describes the grounds for the operation. The sanctions decision sets out the position of the Council of the EU. The company’s responses make it possible to verify exactly what it is contesting.

Each source answers its own part of the question. Together, they provide a more comprehensive picture than a list of high-profile names. Yet even taken together, they do not obviate the need to prove each individual connection.

The main unresolved question is who actually retained the ability to manage the infrastructure and generate revenue from it following the corporate changes. The answer requires information on control, the transfer of assets and the actual fulfilment of contracts. It is precisely these factors that make it possible to distinguish a standard sale of a business from an arrangement designed to preserve the interests of the former owners.

When a criminal service disappears from one address, it is important to understand whether its technical and financial foundations have also vanished. The story of Stark, the Nekuliti brothers and MIRhosting shows why such an investigation must go beyond the website and its logo — right down to the companies, the equipment and the decision-makers.

This article is based on publicly available documents and published investigations, verified as at 15 October 2026. The conclusions of government bodies and researchers are cited with attribution. The views of those involved are set out based on their published responses; the editorial team does not present these responses as having been obtained in response to its own enquiries.

Sources

1. 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/
2. 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/
3. CORRECTIV — an 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. ICIJ Offshore Leaks / Pandora Papers — MORENEHOST LTD and beneficial owner IVAN NEKULITSY
   https://offshoreleaks.icij.org/nodes/240120865
5. Morphisec Labs — investigation into an attack exploiting a VMware vulnerability and the Stark infrastructure, 25 April 2022

An active link to the original is required when reusing materials

https://www.morphisec.com/blog/vmware-identity-manager-attack-backdoor/

6. Companies House — Stark Industries Solutions Ltd, No. 13906017; status and dates of registration
   https://find-and-update.company-information.service.gov.uk/company/13906017
7. Companies House — directors of Stark Industries Solutions Ltd
   https://find-and-update.company-information.service.gov.uk/company/13906017/officers
8. Companies House — persons with significant control over Stark Industries Solutions Ltd
   https://find-and-update.company-information.service.gov.uk/company/13906017/persons-with-significant-control
9. MIRhosting — biographical details about Andrei Nesterenko and his collaboration with the piano competition, 22 February 2026
   https://mirhosting.com/mirhosting-international-piano-competition-enschede-livestream
10. MIRhosting — statement in response to media reports, 22 May 2026
    https://mirhosting.com/verklaring-mirhosting-naar-aanleiding-van-recente-mediapublicaties
11. Recorded Future / Insikt Group — One Step Ahead: Stark Industries Solutions Pre-empts EU Sanctions, 27 August 2025
    https://www.recordedfuture.com/research/one-step-ahead-stark-industries-solutions-preempts-eu-sanctions
12. Council of the EU – sanctions against Stark Industries and the Nekuliti brothers, 20 May 2025
    https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russian-hybrid-threats-eu-lists-further-21-individuals-and-6-entities-and-introduces-sectoral-measures-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-international-partners/
13. Council of the EU – Regulation 2026/2257 of 8 October 2026, Articles 27–28; official text in the BOE
    https://www.boe.es/buscar/doc.php?id=DOUE-L-2026-81528
14. MIRhosting — our own analysis of traffic for October–November 2025, published on 2 June 2026
    https://mirhosting.com/the-november-2025-danish-election-attacks-what-our-own-network-data-shows
15. 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

Use of materials

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

Original publication

https://kartel-khimprom.com/en/article/ivan-and-yuri-nekuliti-andrei-nesterenko-servers-sanctions-and-the-dark-side-of-web-hosting/