

Threat Research:

European Union Sanctions Force Stark Industries Solutions Ltd. to Rebrand Again

01 Executive Summary

On May 20, 2025, the European Union imposed sanctions under Council Regulation (EU) 2024/2642 against Ivan Neculiti and Iurie Neculiti, citing their role in supporting Russia's hybrid operations through cyberattacks and coordinated disinformation campaigns. The sanctions include asset freezes, travel bans, and a prohibition on EU entities making funds or resources available to them. Their company, Stark Industries Solutions Ltd., was designated for providing web hosting infrastructure that enabled Russian state-sponsored and affiliated actors to obscure malicious activity targeting the EU and its allies.

Ivan Neculiti, listed as the owner, and Iurie Neculiti, the CEO, operated Stark Industries as a UK-registered maildrop hosting provider with a global footprint. The company has played a central role in facilitating malware operations, influence campaigns, and cybercrime. This report discusses the Neculitis' evolving infrastructure across multiple rebrands history PQ Hosting (AS43624), Weiss Hosting Group (AS44774), Stark Industries (AS44477), and PQ Hosting Plus (AS44477) following the sanctions and the impact on Ivanov Vitaliy Sergeevich (AS48031, previously known as XSERVER-UA), with whom they shared infrastructure (leasing) linked to Moldova and the pro-Russian region of Transnistria.

In this piece, we explore the complex dynamics at play in the Transnistria region, take a closer look at the sanctions against Stark Industries, and take a deep dive into how Stark Industries operates and its links with cybercriminal organizations and APT groups. We leverage the Augur Preemptive Cybersecurity platform to uncover associations between infrastructure used in bulletproof hosting. Finally, we share a few recommendations for dealing with bulletproof hosters.

02 Complex Dynamics in the Transnistria Region

Moldova is facing serious national security challenges as it struggles with political instability, weak institutions, and an underfunded defense system. Moldova is also under growing pressure from Russia, which employs tactics such as cyberattacks, disinformation campaigns, and political influence operations. These efforts aim to disrupt Moldova's efforts to align more closely with the European Union and foster instability and division within the country.

A significant element in Russia's cyber activities appears to be rooted in Transnistria, a breakaway region with close ties to Russia. Notably, a company that operated from Transnistria, PQ Hosting, has been identified as a central node in orchestrating Russian information attacks targeting Europe. This company provided infrastructure to pro-Russian hacker groups involved in a range of malicious activities, including distributed denial-of-service (DDoS) attacks, espionage, and the spread of disinformation.

The owners of PQ Hosting eventually rebranded as Weiss Hosting Group, and later as Stark Industries Solutions, a company now registered in the United Kingdom. Their infrastructure has been repeatedly associated with threat activity and has been accused by various reporting entities of providing so-called "bulletproof hosting" services that are resilient to takedown requests and often exploited by threat actors to operate with relative anonymity. The persistent use of this infrastructure by malicious actors underscores the potential role of permissive hosting environments in facilitating cybercriminal operations across specific regions.

Transnistria's lack of comprehensive data protection laws contributes to this environment. This absence of robust privacy regulations creates a permissive space for entities involved in cybercrime, as there are fewer legal hurdles and less oversight compared to jurisdictions with stricter cyber laws. Other hosting providers, such as AlexHost, which has previously been linked to Transnistria, have also been associated with bulletproof hosting. Reporting by Intel 471 highlights AlexHost as an example of infrastructure leveraged by cybercriminals due to its permissive policies and resistance to takedown.

03 Sanctions Against the Neculitis and Regulatory Action

The European Union has imposed sanctions on Iurie Neculiti and Ivan Neculiti under Council Regulation (EU) 2024/2642, which targets individuals and entities involved in Russia's destabilizing hybrid operations.

Both Iurie and Ivan Neculiti are now subject to restrictive EU measures. These typically include asset freezes and a ban on making funds or economic resources available to them. As individuals, they are also likely facing travel bans, preventing entry into or transit through EU member states.

Iurie Neculiti is identified as the CEO of Stark Industries Solutions Ltd., while Ivan Neculiti is listed as the owner of the same company.

Stark Industries Solutions Ltd., registered in the United Kingdom, provides global web hosting services. According to the EU, the company has supported Russian state-sponsored and affiliated actors by offering services designed to conceal coordinated information manipulation, cyberattacks, and other malicious activity from European authorities. These services have reportedly been used to facilitate disinformation and influence operations, launch cyberattacks, including denial-of-service campaigns, and support criminal groups aligned with Russian state interests.

By enabling this infrastructure, the Neculitis are considered to be aiding Russian actions that undermine democracy, stability, and the rule of law in the EU, its member states, and beyond. These sanctions took effect around May 20, 2025, as part of the EU's broader efforts to counter Russia's hybrid threats and malign influence.

The company also accepts cryptocurrency payments, which further obscure attribution and financial tracing. Despite claims of occasional cooperation with researchers, Stark Industries has been repeatedly linked to cybercrime groups such as FIN7, and its infrastructure continues to be associated with APTs and ransomware operators.

04 Infrastructure Rebranding

Autonomous System Numbers (ASNs) associated with the Neculitis reflect a consistent pattern of rebranding and obfuscation, often used to evade scrutiny and takedown efforts. This evolution began with AS43624, known as PQ Hosting, which operated primarily out of Moldova and the breakaway region of Transnistria. PQ Hosting was widely known for offering bulletproof hosting services, resilient infrastructure often used by cybercriminals and state-aligned threat actors due to its resistance to takedown requests.

As pressure mounted, the infrastructure transitioned to AS44774, known as Weiss Hosting Group, a likely rebrand of PQ Hosting. This ASN maintained similar operational patterns and was closely tied to Ivan Neculiti, continuing the same hosting practices under a new name.

Next came AS44477, Stark Industries Solutions Ltd., the most prominent brand associated with the Neculitis. While registered in the United Kingdom, the company retained strong backend ties to Moldova and Russia. Stark Industries gained recognition for offering abuse-resistant VPS infrastructure, fast-rotating IP pools, and services specifically designed for use by advanced persistent threats and ransomware groups.

Following EU sanctions in May 2025, Stark Industries' infrastructure underwent another transformation. AS44477 was effectively rebranded again as PQ Hosting Plus, which inherited many of Stark's previous IP prefixes. The group demonstrates clear operational continuity despite regulatory action, highlighting its efforts to remain functional while also shielding itself from potential prosecution.

Additionally, AS48031, which goes by the name Ivanov Vitaliy Sergeevich (previously known as XSERVER-UA), played a key supporting role. Based in Moldova, this ASN had a history of announcing IP ranges on behalf of Stark Industries. However, following the sanctions, AS48031 reassigned prefixes totally back to PQ Hosting Plus, likely in an attempt to distance itself from the sanctioned infrastructure and avoid secondary scrutiny.

05 Involvement in the Russia—Ukraine Conflict

Stark Industries (AS44477) became operational shortly before Russia's full-scale invasion of Ukraine in 2022. From the outset, it has been closely tied to infrastructure used in cyber operations that support Russian strategic interests. Several threat actors leveraged Stark's services to carry out attacks aligned with this broader geopolitical conflict.

Blue Charlie, also known as Star Blizzard, exploited Stark-hosted infrastructure for credential harvesting and spear-phishing campaigns aimed at NGOs and government agencies. Similarly, Sandworm, affiliated with Russia's GRU Unit 74455, used the same infrastructure to support disruptive cyberattacks across Eastern Europe.

Sandworm, a highly sophisticated unit associated with Russia's GRU, also relied on Stark-hosted infrastructure for cyber operations. This included their involvement in the 2023 cyberattack against the Ukrainian news agency Ukrinform. In parallel, Stark Industries served as a platform for hosting VPNs and proxy services that facilitated disinformation campaigns and broader espionage efforts.

06 Nation-State and Ransomware Actor Usage

Stark Industries Solutions (AS44477) has been used by a range of threat actors, spanning both state-sponsored groups and financially motivated ransomware operators. The infrastructure's abuse-resistant nature has made it particularly attractive for high-impact cyber operations.

The financially motivated group FIN7 deployed Stark-based servers for phishing operations and malware distribution. Ransomware operators, including LockBit and Conti, relied on Stark's bulletproof VPS hosting for staging payloads, running command-and-control nodes, and exfiltrating stolen data.

PQ Hosting (AS43624), another infrastructure node linked to the Neculiti network, was also used by APT28 (AKA Fancy Bear) for espionage activities. Ransomware gangs like REvil and DarkSide used PQ's infrastructure to host negotiation portals and payload servers, suggesting a shared or overlapping ecosystem.

07 Augur Data confirming public data

Our preemptive data shows that AS44477 (Stark Industries Solutions) has predominantly hosted sophisticated Russian cyber actors and malware families. This highlights the central role this infrastructure has played in enabling pro-Russian cyber activity targeting Europe, Ukraine, and other regions. Russian-aligned threat groups, including Sandworm, APT28 (also known as Fancy Bear), and cybercriminal groups such as FIN7, Conti, and LockBit, have leveraged malware like Qakbot, IcedID, and Ursnif, often delivered through loaders like PrivateLoader and DarkGate. These were supported by post-exploitation frameworks, such as Cobalt Strike and Sliver, which facilitated long-term access and the deployment of ransomware. Pro-Russian hacktivist groups, such as NoName057(16), also relied on AS44477 infrastructure to conduct Distributed Denial-of-Service (DDoS) attacks and propagate influence operations, thereby reinforcing Russia’s hybrid warfare objectives.



AS44477’s abuse-resistant architecture made it a preferred hub for staging command-and-control servers, phishing kits, malware, and VPNs. While Iranian threat actors such as APT35 (Charming Kitten) and APT42 (TA455) also utilized AS44477-linked infrastructure to deploy remote access trojans like Remcos and Agent Tesla, their activity was more narrowly focused on espionage. Similarly, Chinese actors have utilized malware families such as PlugX and ShadowPad, with less direct overlap in infrastructure. Collectively, the repeated use of AS44477 by this range of threat actors highlights how bulletproof hosting ecosystems underpin both global cybercrime and nation-state operations.

As discussed in the Infrastructure Rebranding section, AS48031 leased a subset of their prefixes to Stark Industries and has since been transformed under AS44477 PQ Hosting Plus.

Table 1 shows the prefix 45.39.192.0/24 announced by AS48031, while Figure 2 shows that it is now announced by AS44477.

ASN	CIDR	Updated_at
48031	45.39.192.0/24	2025-03-18 1:34:56
48031	45.39.192.0/24	2025-03-18 2:31:34

Table 1.
Historical BGP
Announcement of
45.39.192.0/24 back
on March 18, 2025

Announced By				
Origin	Origin Registrant	Prefix	Prefix Registrant	
AS44477	PQ HOSTING PLUS S.R.L.	45.39.192.0/24	 	STARK INDUSTRIES SOLUTIONS LTD


Matching Delegations			
Registry	Status	Prefix	CC
arin	allocated	45.38.0.0/15	US 

Figure 1.
New BGP
Announcement of
45.39.192.0/24

08 Conclusion

The case of Stark Industries Solutions illustrates how hosting providers can inadvertently or knowingly become hubs for malicious cyber activity. Through a history of rebranded infrastructure, opaque ownership structures, and permissive hosting practices, the network surrounding this company has attracted threat actors with suspected links to Russian geopolitical objectives.

While proving direct coordination can be difficult, the repeated use of infrastructure linked to Stark Industries Solutions by threat actors involved in cybercrime and influence operations reflects patterns commonly associated with bulletproof hosting services. As detailed by Intel471, such services are designed to shield malicious activity from law enforcement and takedown efforts, making them a persistent enabler of hybrid threats. The EU's recent sanctions underscore growing recognition of the role this infrastructure plays in facilitating cybercriminal and state-aligned operations.

This development also highlights the ongoing challenge of identifying and disrupting abuse-resistant hosting environments that quickly adapt to legal and regulatory pressures. Enhanced visibility, international collaboration, and proactive intelligence-sharing will be essential to mitigating the risks posed by such resilient cyber ecosystems.

09 Recommendations

- ▶ Prioritize preemptive threat intelligence capabilities that detect and flag suspicious infrastructure at the time of registration or first emergence, before it is weaponized. Tools like Augur Security can enhance visibility into emerging ASNs and malicious infrastructure patterns.
- ▶ Build integrated monitoring and alerting pipelines between threat intelligence platforms, DNS data providers, and BGP monitoring services to surface early indicators of rebranded infrastructure.
- ▶ Establish collaborative relationships with ISPs, hosting registrars, and upstream providers to support intelligence-driven takedown and mitigation strategies.
- ▶ Leverage attribution models that combine behavioral clustering, ASN ownership analysis, and hosting characteristics to identify high-risk networks proactively.
- ▶ Expand the use of NetFlow and passive DNS data to uncover obfuscated linkages between sanctioned entities and infrastructure aliases.

10 Sources

Stark Industries Solutions: An Iron Hammer in the Cloud:

<https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud>

Stark Industries: Fueling Russia's Cyber Offensive:

<https://correctiv.org/en/fact-checking-en/2024/05/31/hacks-and-propaganda-meet-the-two-brothers-bringing-russias-cyber-war-to-europe>

EU Sanctions Orgs and Individuals Tied to Russia Disinformation:

<https://therecord.media/eu-sanctions-orgs-individuals-tied-to-russia-disinformation>

OpenSanctions Profile - Neculiti Entities:

<https://www.opensanctions.org/entities/NK-QjxCZxmVmGZjtYMAmRugYX/>

EU Council Regulation (EU) 2024/2642:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500965&qid=1750805035914

EU Council Regulation (EU) 2024/2642:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402642

European Union Sanctions Stark Industries for Enabling Cyberattacks:

<https://www.bleepingcomputer.com/news/security/european-union-sanctions-stark-industries-for-enabling-cyberattacks>

Bulletproof Hosting: A Critical Cybercriminal Service:

<https://intel471.com/blog/bulletproof-hosting-a-critical-cybercriminal-service>