CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 27, 2025

One Step Ahead: Stark Industries Solutions Preempts EU Sanctions

Leaked EU sanctions reported in Moldovan and EU media likely prompted Stark Industries to restructure its network infrastructure, with notable changes observed as early as one month before its designation.

Despite formal EU sanctions, the company re-emerged as THE.Hosting under Dutch entity WorkTitans B.V., sustaining services with minimal disruption.

Threat activity enablers' considerable control over RIPE NCC resources renders sanctions ineffective without multilateral enforcement and meaningful intervention from RIPE.

Executive Summary

Prior to being designated for sanctions by the European Union on May 20, 2025, UK-registered web-hosting provider Stark Industries Solutions Ltd executed a series of infrastructure and organizational changes. Insikt Group assesses this activity to be a strategic effort to preempt impending sanctions and preserve operational continuity. Changes included the registration of a new entity in RIPE, PQ Hosting Plus S.R.L., and, as early as April 10, 2025, the migration of Russian infrastructure to UFO Hosting LLC. Notably, on May 8, 2025, twelve days prior to the sanctions, Moldovan and EU media reported on the forthcoming inclusion of the Neculiti brothers in the next EU sanctions package, citing leaked documentation.

Following the sanctions, Insikt Group observed the rebranding of Stark Industries operations to "THE.Hosting", under the control of Dutch entity "WorkTitans B.V.", and the creation of a new autonomous system, AS209847 (THE), on June 24, 2025. Although the majority of associated infrastructure remains attributable to Stark Industries, these changes likely reflect an attempt to obfuscate ownership and sustain hosting services under new legal and network entities. Insikt Group assesses that the EU's sanctioning of Stark Industries was largely ineffective, as affiliated infrastructure remained operational and services were rapidly re-established under new branding, with no significant or lasting disruption.

This outcome highlights how threat activity enablers (TAEs) — entities that enable malicious cyber activity by providing infrastructure or services leveraged by threat actors — that retain such significant control over RIPE resources, such as Local Internet Registries (LIRs), Autonomous Systems (ASes), and IP prefixes, are particularly well-positioned to rebrand, reallocate infrastructure, and maintain operational continuity in the absence of meaningful intervention by RIPE NCC. More broadly, the case demonstrates the structural resilience of modern TAEs and underscores the need not only for sustained monitoring by network defenders but also for coordinated, cross-border collaboration among policymakers and law enforcement. Regional sanctions alone are insufficient; meaningfully disrupting TAEs operating at the scale of Stark Industries requires a comprehensive, multilateral approach.

Key Findings

- Stark Industries, along with its CEO and owner, was formally sanctioned by the Council of the European Union on May 20, 2025, for enabling Russian state-sponsored cyber operations, including information manipulation, infrastructure for cyberattacks, and other destabilizing hybrid threats against the EU and its partners.
- Stark Industries preempted its EU designation through a series of calculated infrastructure and organizational changes, including the registration of new RIPE entities and the early migration of Russian infrastructure to UFO Hosting LLC.
- On May 29, 2025, nine days after the EU designation, PQ.Hosting publicly rebranded to THE.Hosting, transferring assets and infrastructure to the Dutch-registered entity WorkTitans B.V. RIPE records show IP prefix and ASN transfers aligning with the rebrand, while website updates briefly referenced WorkTitans as the legal entity.
- All transitional entities, PQ Hosting Plus S.R.L., UFO Hosting LLC, and WorkTitans B.V., share RIPE maintainer objects linked to the email address *jama**[@]gmail[.]com*, which Insikt Group attributes to Dmitrii Miasnikov, a known Russian network operator. These maintainer objects were responsible for all associated RIPE organizations.
- Stark Industries' pre- and post-sanctions activities reflect a deliberate, multi-phase restructuring designed to minimize the impact of EU designations while sustaining its role as a threat activity enabler (TAE). Despite sanctions, the entity successfully maintained infrastructure availability and operational continuity under alternative legal and network identities.

The Enduring Challenge of Threat Activity Enablers

The global cybersecurity landscape is increasingly shaped by the proliferation of threat activity enablers (TAEs), which are entities that enable malicious cyber activity by providing infrastructure or services leveraged by threat actors. Some such entities can present as lawful businesses, relying on legal or technical obfuscation to avoid accountability while tolerating varying degrees of malicious activity.

This nuanced descriptor encompasses a broad spectrum of modern enabling services, such as hosting providers who selectively respond to abuse reports or law enforcement requests to maintain plausible deniability, to more traditional bulletproof hosting providers that ignore all oversight.

TAEs that provide hosting services pose significant and enduring challenges for several reasons:

- **Obfuscation and Evasion:** TAEs routinely navigate legal loopholes and use complex corporate structures, shell companies, and distributed infrastructure across multiple jurisdictions to obscure their true ownership and the nature of their services. This makes identification, attribution, and legal action exceedingly difficult for law enforcement and cybersecurity researchers.

- **RIPE Resource Abuse:** Many TAEs maintain strategic control over RIPE (Réseaux IP Européens) resources, including IP ranges, Autonomous Systems (ASs), and associated registration objects, enabling them to manipulate and redistribute network resources at will. This infrastructure control allows TAEs to rapidly rebrand, spin up new entities, and distribute fresh subnets and ASNs, often to evade sanctions or scrutiny.
- **Enabling Diverse Threat Actors:** By providing services such as web hosting, Virtual Private Servers (VPS), Virtual Private Networking (VPN) services, and proxy networks, TAEs can become critical enablers for a wide array of cyber threats. This includes ransomware operators, infostealer campaigns, botnets, state-aligned threat actors, hacktivists, and influence operations. Their services allow threat actors to maintain anonymity, launch attacks, and host malicious content with varying degrees of resiliency against takedown efforts.

Insikt Group has tracked and reported on long-established and emerging TAEs, leveraging Recorded Future's Network Intelligence to assess the concentration of malicious activity relative to the total size of IP space under an ASN's control. This highlights operators whose infrastructure is disproportionately associated with threat activity.

Background

Stark Industries Solutions, a web-hosting provider that has recently drawn international attention due to recent sanctions, has roots deeply embedded in the hosting industry. It has evolved from the individual ventures of its founders to a sophisticated global network.

Stark Industries was officially incorporated in the United Kingdom on February 10, 2022, notably just two weeks prior to Russia's full-scale invasion of Ukraine. The company primarily offers web-hosting services, including VPSs, numerous proxy services, and VPNs. It was founded by brothers Iurie Neculiti and Ivan Neculiti, whose involvement in illicit hosting dates back over a decade, as Ivan's previous web-hosting service, Morenehost, gained notoriety for enabling cyber threats (his ownership was revealed through the Pandora Papers data leak).

Stark Industries Solutions functioned mainly as a pass-through company designed to obscure the true nature of its operations. In effect, transactions with Stark Industries were transactions with PQ.Hosting, though this was not immediately apparent to external parties. Ivan Neculiti characterized Stark Industries as a "white label" brand, enabling resellers to distribute PQ.Hosting's services without direct customer interaction. The Neculiti brothers strategically established companies in Moldova, Russia, and Great Britain, creating a complex corporate structure engineered for obfuscation.

Following the onset of the war in Ukraine, Stark Industries rapidly became a central platform for significant distributed denial-of-service (DDoS) attacks conducted by hacktivist group NoName057(16). Furthermore, Stark Industries' infrastructure was highlighted in early 2024 as central to the resurgence of the financially motivated threat actor FIN7. As late as mid-2025, Insikt Group has continued to observe GrayAlpha, a threat cluster with significant overlap with FIN7, rely on Stark Industries' infrastructure.

On May 20, 2025, the EU sanctioned Stark Industries Solutions Ltd, along with its CEO, Iurie Neculiti, and owner, Ivan Neculiti, for enabling Russian state-sponsored cyber operations, including information manipulation, cyberattacks, and other destabilizing hybrid activities targeting the EU and its partners. Insikt Group tracks Stark Industries Solutions Ltd (referenced hereafter as Stark Industries) and its parent company, PQ.Hosting, as threat activity enablers (TAEs) that enable a multitude of state-sponsored cyber operations linked to Russia, Iran, North Korea, and China, as well as cybercriminal groups.

Threat Analysis

EU Sanctions Stark Industries

On May 20, 2025, the Council of the European Union sanctioned internet service provider (ISP) Stark Industries, along with its CEO, Iurie Neculiti, and owner, Ivan Neculiti. Insikt Group tracks Stark Industries and its parent organization, PQ.Hosting, as TAEs, enabling a multitude of state-sponsored cyber operations linked to Russia, Iran, North Korea, and China, as well as cybercriminal groups. Insikt Group notes that although PQ.Hosting was referenced within the sanctions multiple times alongside Stark Industries, the company itself was not sanctioned. Details of the sanctioned company and individuals are outlined in **Tables 1** and **2**.

Company	Registration Number	Address	Websites
Stark Industries Solutions Ltd.	13906017	71-75 Shelton Street, Covent Garden, London, UK	*pq[.]hosting* *stark-industries[.]solutions*

Table 1: *Stark Industries Solutions sanctions details (Source: EU Council)*

Name	Function	Nationality	Address	Place of Birth
Iurie Neculiti	CEO of Stark Industries	Moldovan	71-75 Shelton Street, Covent Garden, London, United Kingdom	Bender, Republic of Moldova
			Chisinau, Republic of Moldova	
Ivan Neculiti	Owner of Stark Industries	Moldovan	71-75 Shelton Street, Covent Garden, London, United Kingdom	Bender, Republic of Moldova
			Chisinau, Republic of Moldova	

Table 2: *CEO and owner of Stark Industries Solutions sanctions details (Source: EU Council)*

The EU attributed Stark Industries' infrastructure to enabling various Russian state-sponsored and affiliated threat actors to conduct destabilizing activities, including information manipulation, interference, and cyberattacks against the European Union and third countries. Furthermore, Insikt Group's 2024 Malicious Infrastructure Report highlighted Stark Industries' infrastructure as one of the top services enabling global cyber threats (see **Figure 1**). To view malware samples that exhibit network connections to Stark Industries' infrastructure, queries are available in **Appendix A** for Recorded Future's Malware Intelligence module.

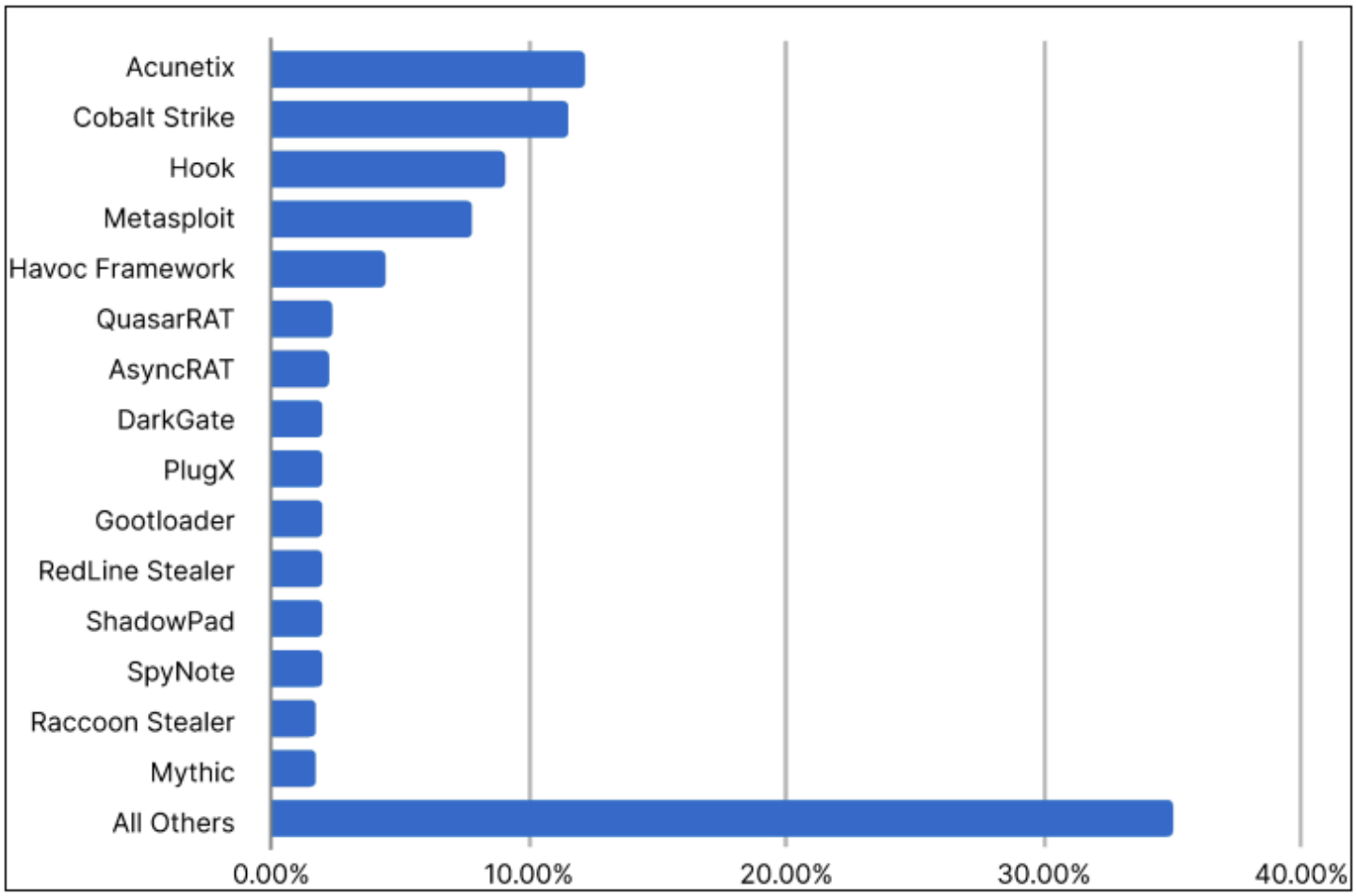

Figure 1: *Top fifteen validated malware families on Stark Industries ASNs in 2024 (Source: Recorded Future)*

Timeline of Events

The following timeline is based on Insikt Group's analysis conducted between May 16, 2025, and June 24, 2025. It outlines key events surrounding the EU's sanctioning of Stark Industries, including pre-sanctions reporting, early infrastructure shifts, and post-designation rebranding.

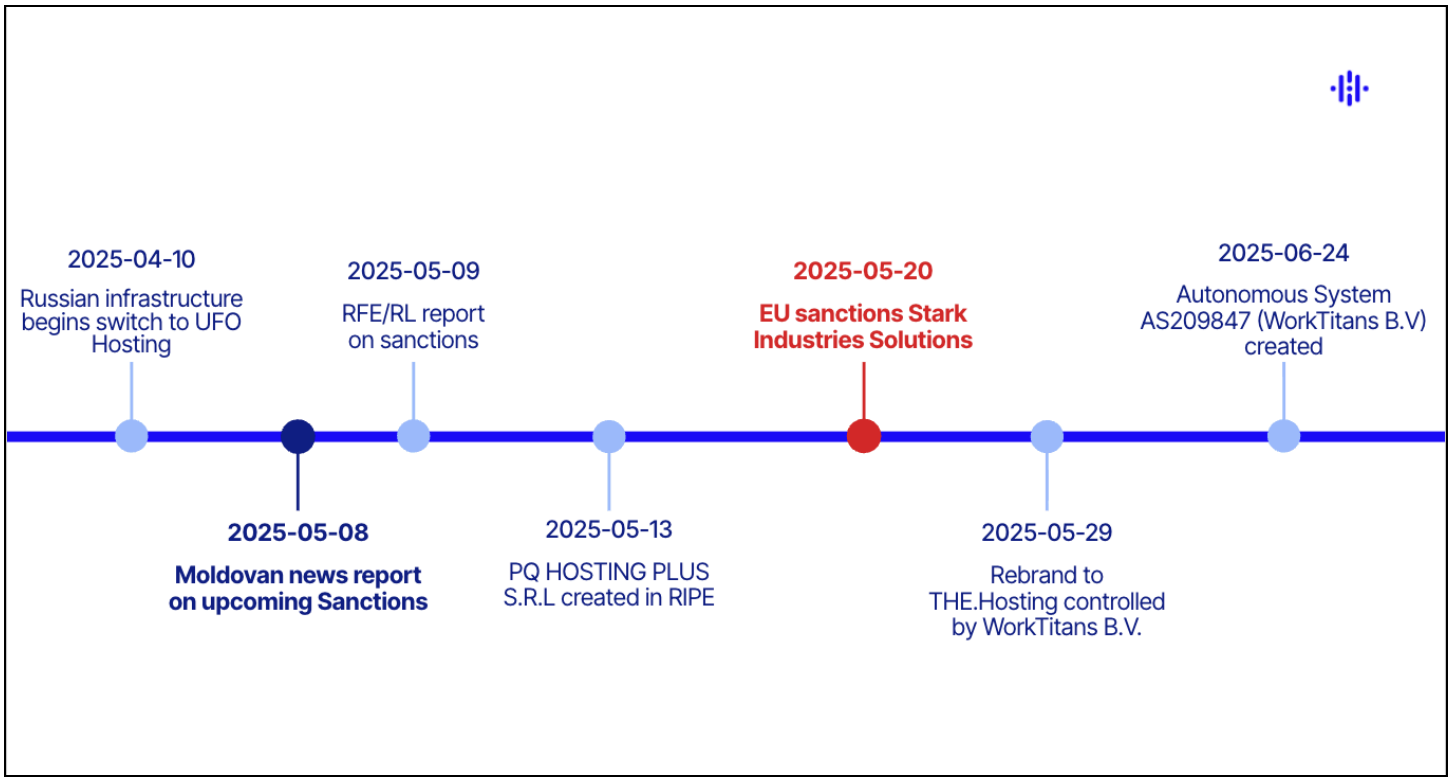

Figure 2: *Timeline of events observed by Insikt Group (Source: Recorded Future)*

The sequence of events indicates that Stark Industries and its affiliated entities likely anticipated forthcoming EU sanctions, potentially as early as April 2025. Public reporting in Moldovan and EU media beginning in early May is highly likely to have triggered further operational shifts, including the creation of new corporate structures and early-stage infrastructure migration. These actions, occurring days before the official designation, suggest a deliberate attempt to mitigate the impact of sanctions and preserve the continuity of hosting services under alternative branding and network ownership.

Pre-Sanctions

Exposure in Moldovan and EU Press

On May 8, 2025, the Moldovan arm of Radio Free Europe/Radio Liberty (RFE/RL) revealed that two Moldovan nationals, Ivan and Iurie Neculiti, founders of Stark Industries, were slated for inclusion in the EU's next sanctions package targeting individuals involved in Russia's hybrid warfare campaign. The article cited direct access to a leaked EU document listing proposed designations, which accused the Neculiti brothers of enabling Russian state-sponsored destabilizing activities against the EU and its partners through their web-hosting company. A follow-up article released by RFE/RL's central newsroom on May 9, 2025, further confirmed the proposed sanctions and framed them within the broader sanctions package under consideration by the European Commission.

Infrastructure Updates

On May 16, 2025, Insikt Group observed that the Autonomous System Number (ASN) AS44477, previously registered to Stark Industries, had been transferred to a newly created RIPE organization in the name of its parent company, PQ Hosting Plus S.R.L., under RIPE identifier ORG-PHPS1-RIPE. This organization object was created just three days prior, on May 13, 2025, following RFE/RL's reporting of the upcoming EU sanctions package (see **Figure 3**).

```
organisation:    ORG-PHPS1-RIPE
org-name:        PQ HOSTING PLUS S.R.L.
country:         MD
org-type:        LIR
address:         str. Spartacus 23
address:         MD2024
address:         Chisinau
address:         MOLDOVA, REPUBLIC OF
phone:           +37369933122
e-mail:          lir[@]pq[.]hosting
remarks:
remarks:         ************************************************
remarks:         * For spam/abuse/security issues please contact *
remarks:         * abuse[@]pq[.]hosting *
remarks:         * The contents of your abuse email will be *
remarks:         * forwarded directly on to our client for *
remarks:         * handling. *
remarks:         ************************************************
remarks:
remarks:         ************************************************
remarks:         * Any questions on Peering/Routing please send to *
remarks:         * noc[@]pq[.]hosting *
remarks:         ************************************************
remarks:
remarks:         ************************************************
remarks:         * Any police request please send to *
remarks:         * police[@]pq[.]hosting *
remarks:         ************************************************
remarks:
admin-c:         PQHS
tech-c:          PQHS
abuse-c:         PQHS371
mnt-by:          RIPE-NCC-HM-MNT
mnt-by:          PQHS-MNT
created:         2025-05-13T11:20:28Z
last-modified:   2025-05-21T23:14:18Z
source:          RIPE
mnt-ref:         PQHS-MNT
mnt-ref:         MEREZHA-MNT
mnt-ref:         IP-RIPE
```

Figure 3: *RIPE organization record ORG-PHPS1-RIPE (Source: RIPE DB)*

Subsequent analysis initially linked the new organization to UFO Hosting LLC, a Russia-based internet service provider (ISP), via a shared email address, *jama**[@]gmail[.]com*, contained within the organization's new RIPE maintainer object, PQHS-MNT. However, upon analyzing announcements from

UFO Hosting's ASN, AS33993 (UFO-AS), it became apparent that Stark Industries was seemingly leveraging the provider to announce its Russian IP prefixes (see **Figure 4**).

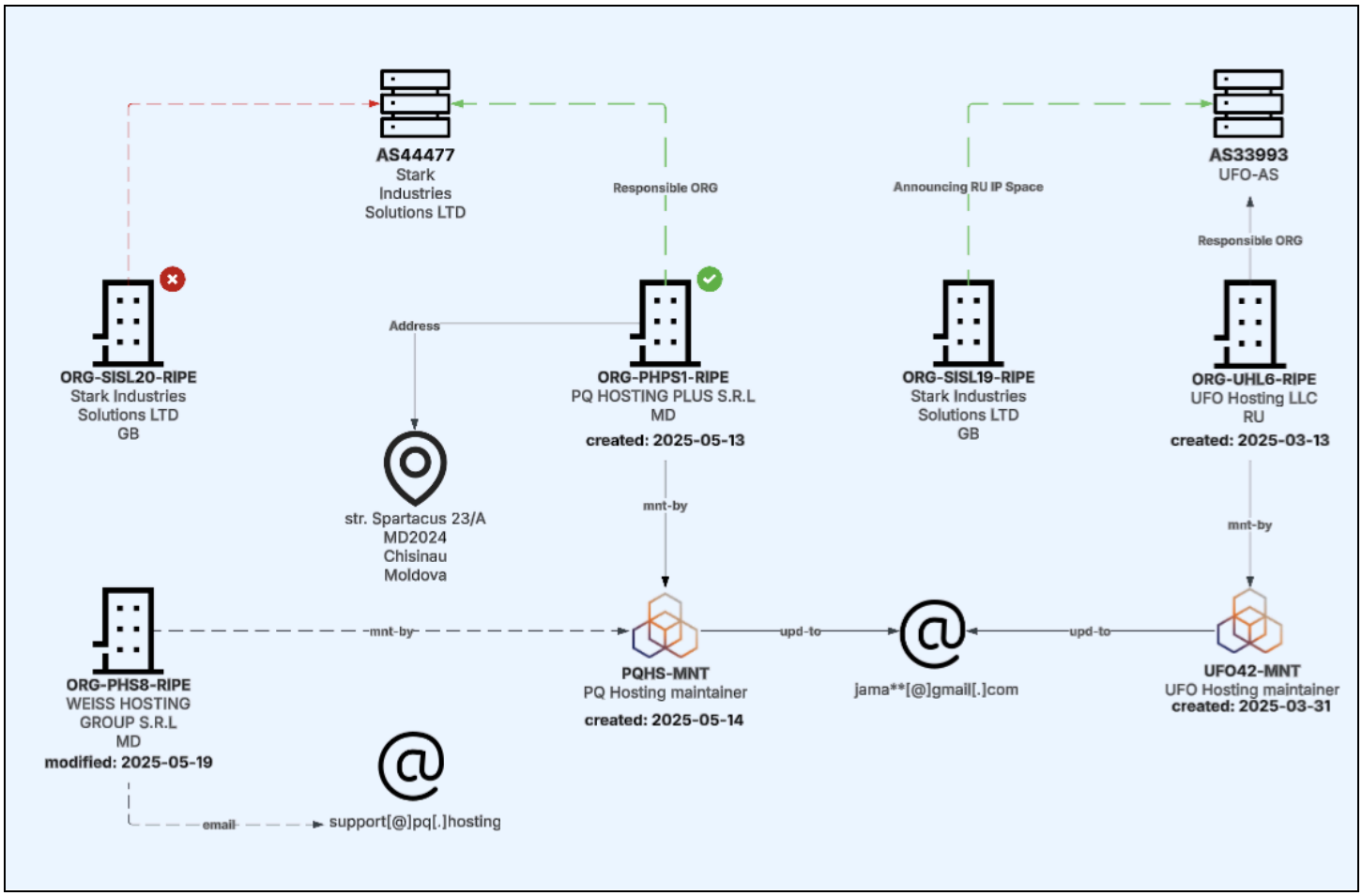

Figure 4: *Pre-sanction infrastructure changes as of May 19, 2025 (Source: Recorded Future / RIPE DB)*

UFO Hosting

UFO Hosting is a Russia-based ISP that was first registered with RIPE on March 13, 2025, under the RIPE identifier ORG-UHL6-RIPE. Russian company registration documents list Savushkin Mikhail Yuryevich as the owner and the registration date as February 18, 2025.

The company offers VPS/VDS and dedicated server hosting via its website *ufo[.]hosting*. The website's user agreement section suggests the company is officially registered under the name YuFO Hosting (ЮФО Хостинг) in Moscow (see **Figure 5**).

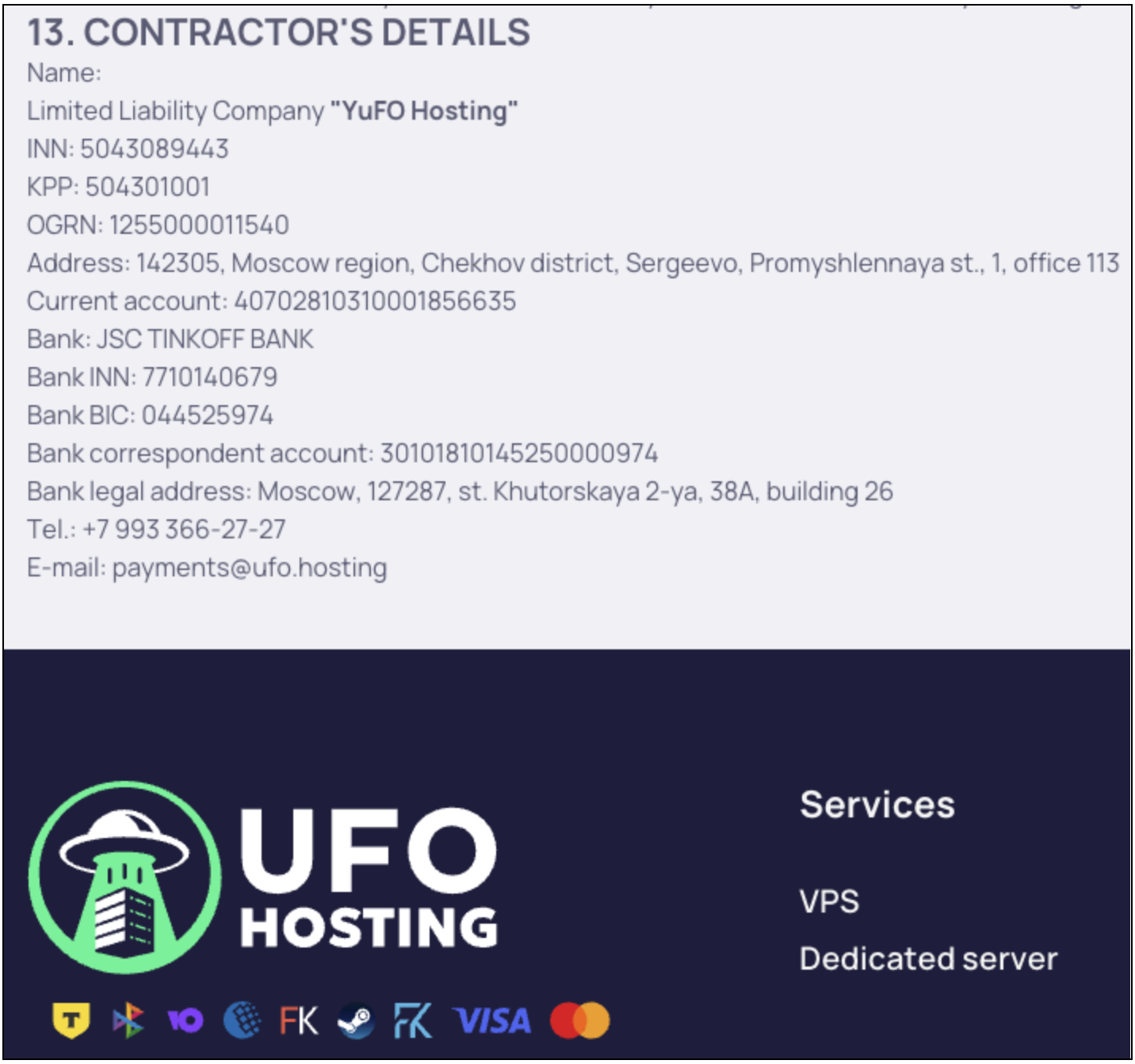

Figure 5: *UFO Hosting website user agreement page (Source: ufo[.]hosting)*

As of May 16, 2025, AS33993 (UFO-AS) announced 21 IP prefixes (see **Appendix B**). Insikt Group identified that all prefixes directly assigned to UFO Hosting's RIPE organization (ORG-UHL6-RIPE) were transferred from Stark Industries. Most of these transfers occurred on April 13, 2025 (see **Figure 6**).

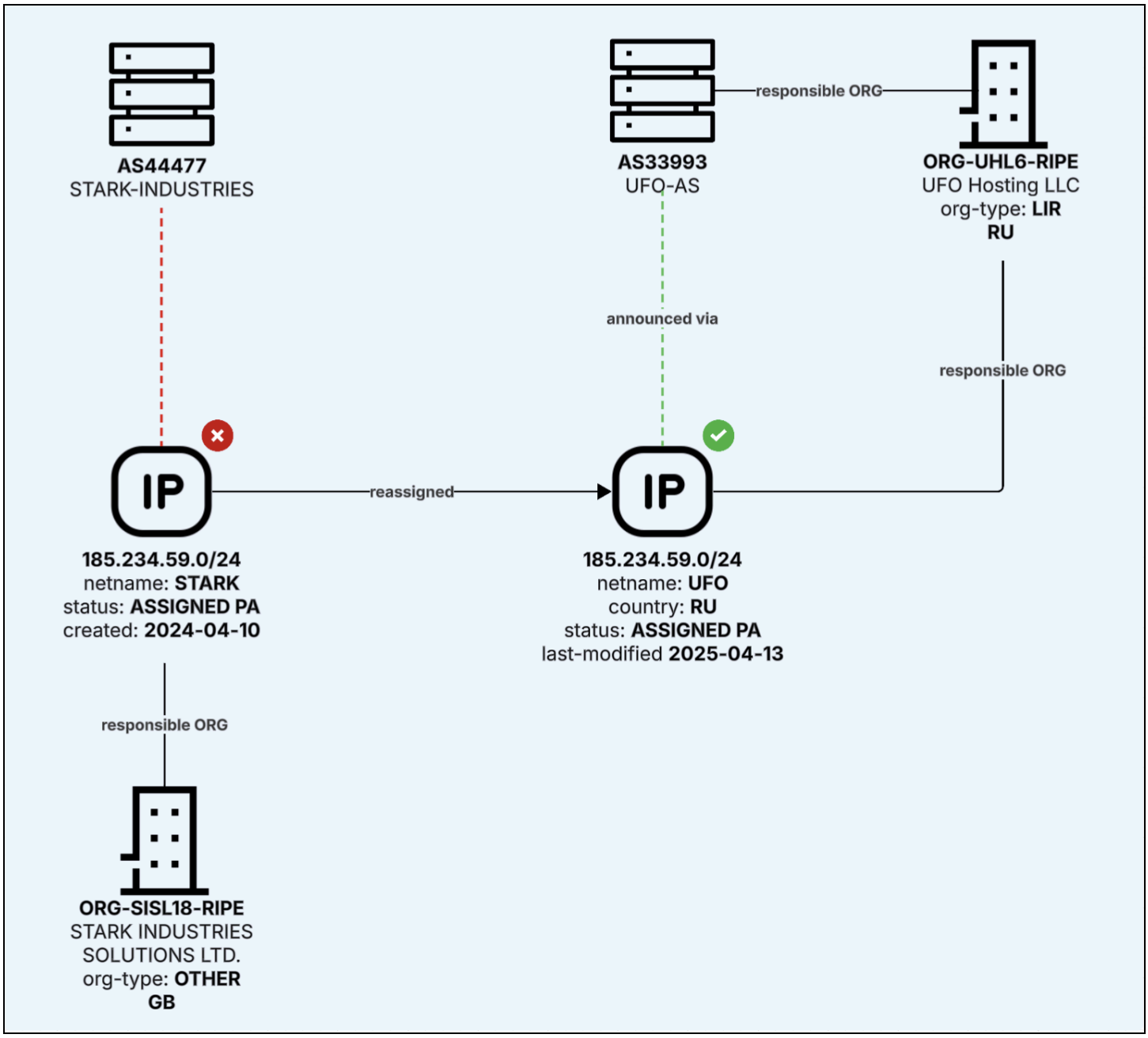

Figure 6: *Example of IP prefix transfer from Stark Industries to UFO Hosting (Source: Recorded Future / RIPEstat)*

Insikt Group also identified several domains associated with Stark Industries and PQ.Hosting infrastructure resolving indirectly to IP addresses announced and controlled by UFO Hosting, further signaling an operational migration. While public DNS resolution showed these domains resolving to StormWall s.r.o DDoS protection endpoints, reverse DNS analysis of the underlying IP space revealed matching domain references on IP addresses transferred from Stark Industries (see **Table 3**).

domain	IP	ASN	ISP
bill-migration-db[.]stark-industries[.]solutions	*45[.]121[.]14[.]142*	AS33993	UFO Hosting LLC
pq-ru[.]digitalvpn[.]org	*45[.]144[.]31[.]195*	AS33993	UFO Hosting LLC
pq[.]company	*45[.]67[.]230[.]222*	AS33993	UFO Hosting LLC
registry[.]pq[.]hosting	*45[.]67[.]230[.]171*	AS33993	UFO Hosting LLC
russia[.]stark-industries[.]solutions	*94[.]131[.]113[.]248*	AS33993	UFO Hosting LLC

Table 3: *Stark Industries and PQ.Hosting domains resolving to UFO Hosting IP addresses (Source: Recorded Future)*

Insikt Group assesses with high confidence that UFO Hosting was established or repurposed as a vehicle for Russia-based infrastructure and clientele, providing a sanctions-resilient platform that enabled Stark Industries to discreetly migrate assets and maintain operational continuity ahead of EU enforcement.

Post-Sanctions

Rebrand to THE.Hosting

On May 29, 2025, nine days after the EU formally sanctioned Stark Industries, its parent company, PQ.Hosting, announced a full rebranding and legal transition to a newly created entity, THE.Hosting. In a public statement, PQ.Hosting declared that the company had ceased to exist "as a legal entity and operational structure," and that all assets, infrastructure, and services had been transferred to THE.Hosting, which would henceforth operate under new ownership and management (see **Figure 7**).

Figure 7: *Rebranding announcement on THE.Hosting's new website (Source: the[.]hosting)*

The rebranded website, operating under a new domain, *the[.]hosting*, referenced WorkTitans B.V. as the legal entity behind THE.Hosting (See **Figures 8** and **9**). Insikt Group notes that as of June 24, 2025, THE.Hosting removed any reference to WorkTitans from its website.

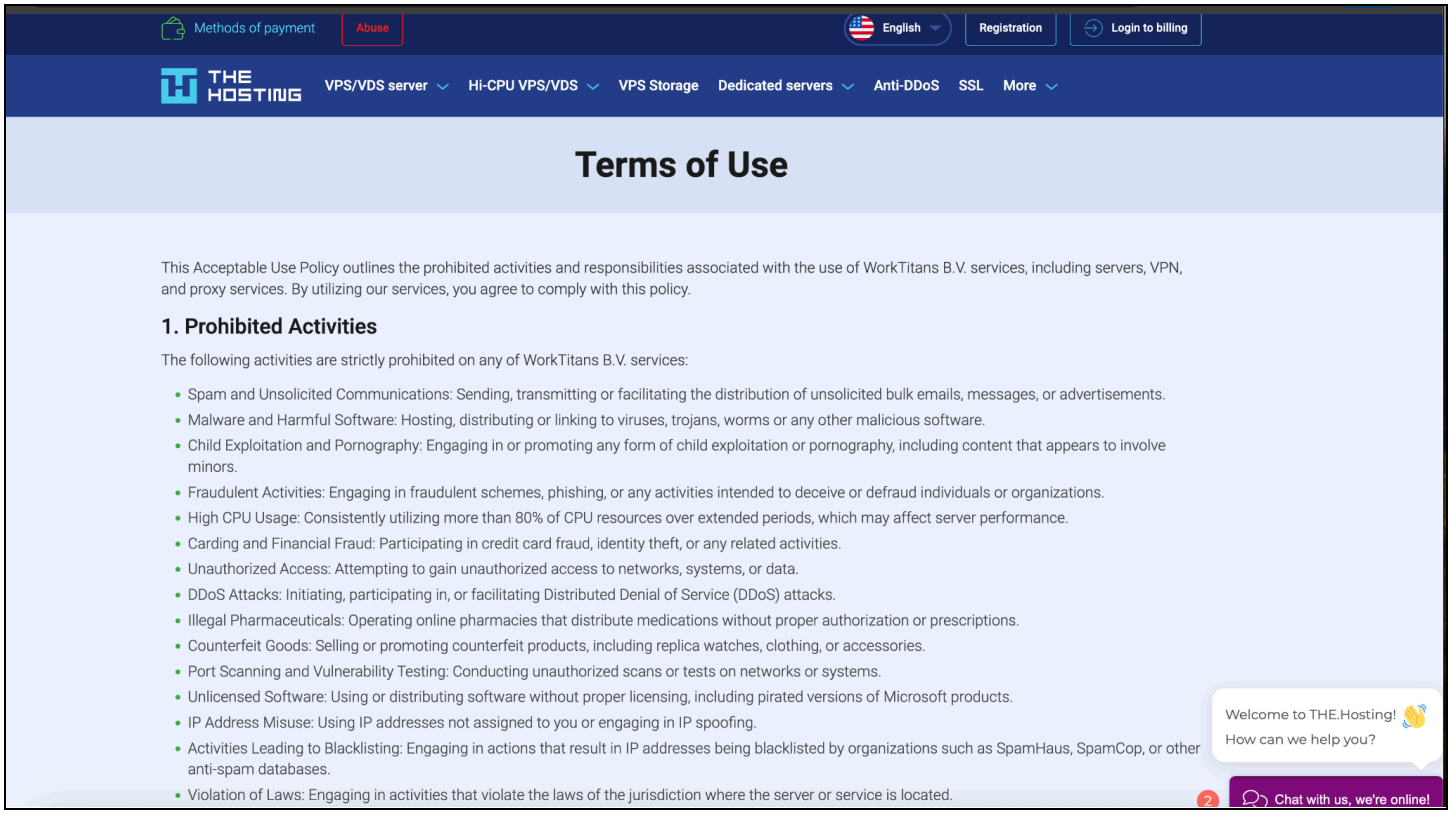

Figure 8: *THE.Hosting's terms of use web page (Source: Archive[.]org)*

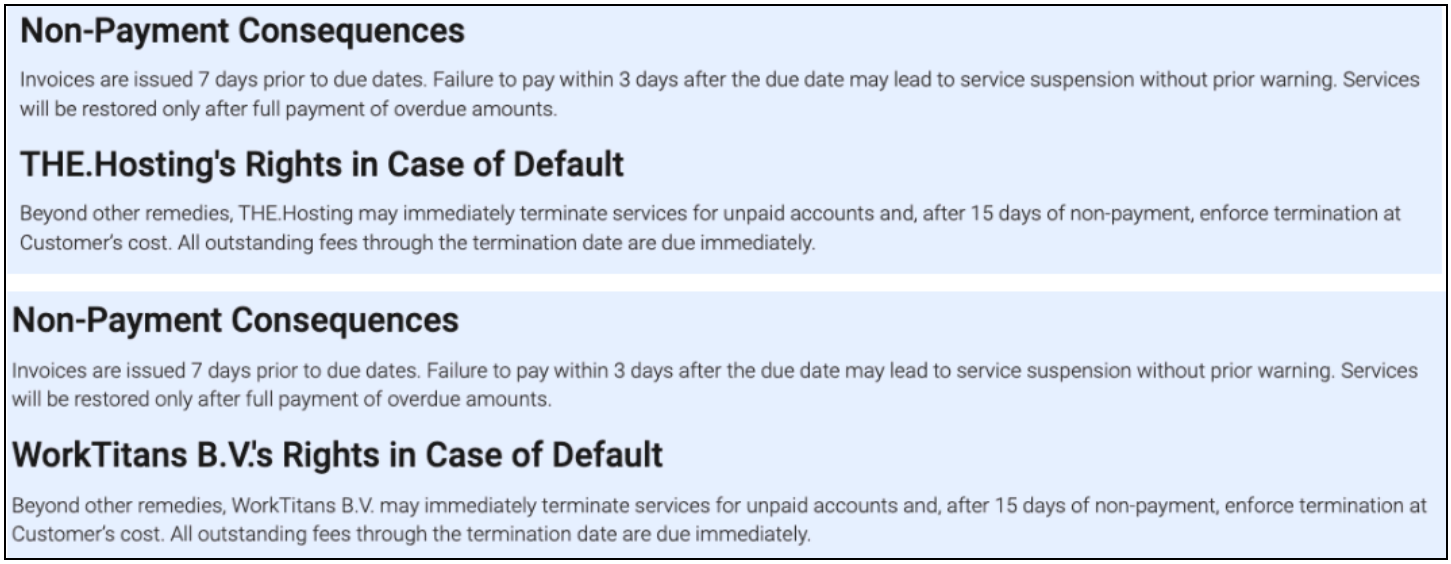

Figure 9: *THE.Hosting's terms of use, removing reference to WorkTitans B.V. (Top) and THE.Hosting's previously observed terms of use page (Bottom) (Source: Archive[.]org)*

WorkTitans B.V.

WorkTitans is a Netherlands-based company ostensibly registered and presenting as a recruitment firm, an affiliation that bears no logical connection to the hosting sector. This clear misalignment strongly suggests that Stark Industries used WorkTitans as its new Western corporate entity to obscure its continuity of control and insulate its rebranded infrastructure from sanctions. WorkTitans' website, *worktitans[.]nl*, displayed minimal functionality, with vague information about the company (see **Figure 10**) and a broken vacancy search page.

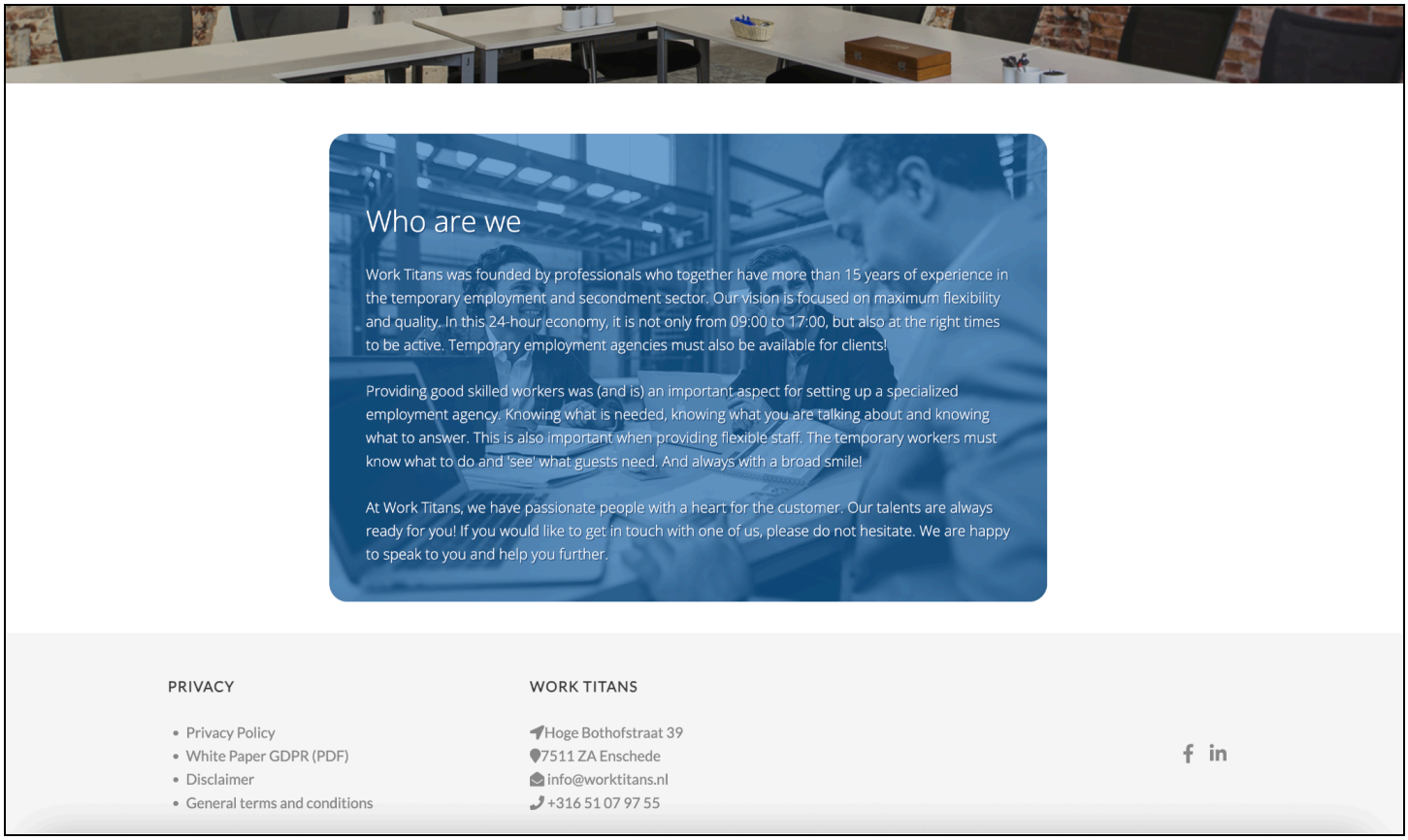

Figure 10: *WorkTitans web page (Source: worktitans[.]nl)*

Infrastructure Updates

Insikt Group observed further changes to Stark Industries' infrastructure between May 29 and June 23, 2025, coinciding with the public rebranding of PQ.Hosting to THE.Hosting and the emergence of a new corporate vehicle, WorkTitans.

On May 29, 2025, Insikt Group observed IP prefixes previously attributed to Stark Industries Solutions began transferring to a newly registered RIPE organization object under the name WorkTitans B.V. Its corresponding RIPE object, ORG-THE3-RIPE, was created on May 28, 2025, the day before the public

rebrand (see **Figure 11**).

```
Abuse contact info: abuse[@]the[.]hosting

organisation:     ORG-THE3-RIPE
org-name:         WorkTitans B.V.
org-type:         OTHER
address:          Hoge Bothofstraat 39, 7511 ZA Enschede, Netherlands
country:          NL
e-mail:           noc[@]the.hosting
abuse-c:          THE666
mnt-ref:          THE-HOSTING-MNT
mnt-ref:          MEREZHA-MNT
mnt-by:           THE-HOSTING-MNT
created:          2025-05-28T17:30:07Z
last-modified:    2025-05-29T00:51:07Z
source:           RIPE
```

Figure 11: *RIPE organization record ORG-THE3-RIPE (Source: RIPE DB)*

Insikt Group continued to monitor the transfer of IP prefixes to WorkTitans between May 29 and June 24, 2025, observing a new netname of THE-HOSTING. Further analysis of historical WHOIS records showed a clear progression — from initial assignment to Stark Industries to reassignment to PQ Hosting Plus S.R.L — leading up to the EU sanctions and subsequent transfer to WorkTitans following the rebrand (see **Figure 12**).

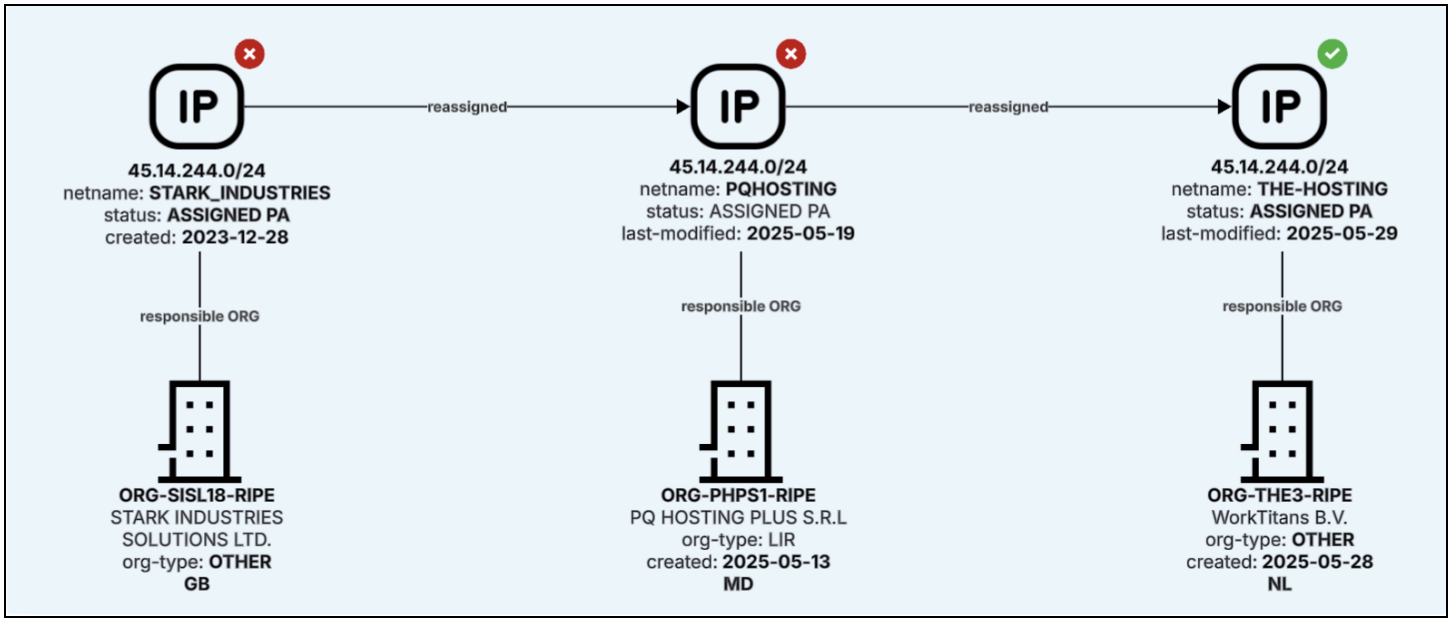

Figure 12: *WHOIS history for IP prefix 45[.]14[.]244[.]0/24 (Source: Recorded Future / RIPEstat)*

In parallel with the observed prefix transfers, Insikt Group also tracked changes to ASN AS44477, registered initially to Stark Industries Solutions. While the responsible organization was updated to PQ Hosting Plus S.R.L., the ASNs name field was sequentially modified, first to reflect PQ.Hosting and, later, THE-HOSTING, aligning with the broader infrastructure rebrand (see **Figure 13**).

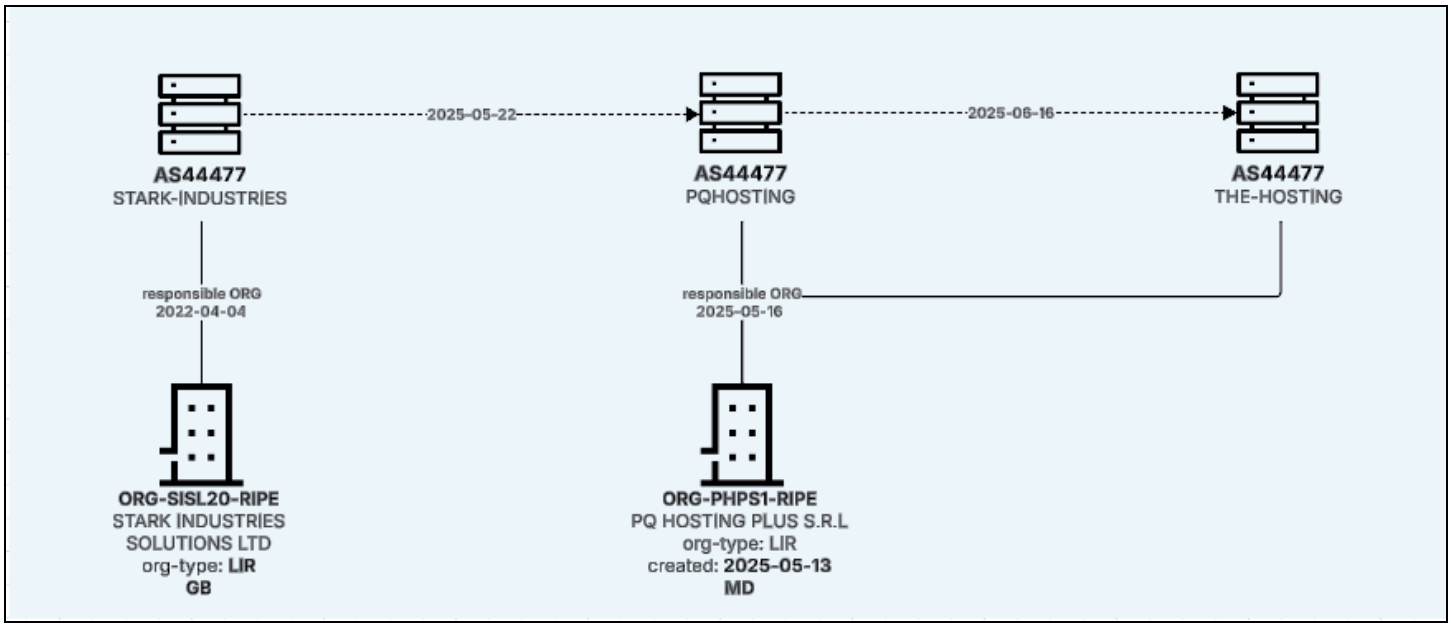

Figure 13: *RIPE AS record history for AS44477 (Source: Recorded Future / RIPEstat)*

Between June 23 and June 24, 2025, Insikt Group identified the registration of a new Local Internet Registry (LIR) under the name WorkTitans B.V., along with a corresponding ASN, AS209847 (THE), further consolidating the rebrand under new RIPE organization object ORG-WB96-RIPE (See **Figures 14** and **15**). AS209847 announced 21 IP prefixes as of August 4, 2025 (See **Appendix C**).

```
Abuse contact info: abuse[@]the[.]hosting

Organisation:    ORG-WB96-RIPE
org-name:        WorkTitans B.V
country:         NL
org-type:        LIR
address:         Hoge Bothofstraat 39
address:         7511 ZA
address:         Enschede
address:         NETHERLANDS
phone:           +31532060000
e-mail:          lir[@]the.hosting
admin-c:         THMC1-RIPE
tech-c:          THMC1-RIPE
abuse-c:         AR78445-RIPE
mnt-ref:         THE-HOSTING-MNT
```

```
mnt-by:          RIPE-NCC-HM-MNT
mnt-by:          THE-HOSTING-MNT
created:         2025-06-23T11:10:15Z
last-modified:   2025-06-23T11:10:16Z
source:          RIPE
```

Figure 14: *RIPE organization record ORG-WB96-RIPE (Source: RIPE DB)*

```
Responsible organisation: WorkTitans B.V
Abuse contact info: abuse[@]the[.]hosting

aut-num:         AS209847
as-name:         THE
org:             ORG-WB96-RIPE
import:          from AS52000 accept ANY
export:          to AS52000 announce AS209847:AS-THE
import:          from AS49434 accept ANY
export:          to AS49434 announce AS209847:AS-THE
import:          from AS8285 accept ANY
export:          to AS8285 announce AS209847:AS-THE
import:          from AS9002 accept ANY
export:          to AS9002 announce AS209847:AS-THE
import:          from AS174 accept ANY
export:          to AS174 announce AS209847:AS-THE
import:          from AS1299 accept ANY
export:          to AS1299 announce AS209847:AS-THE
import:          from AS6939 accept ANY
export:          to AS6939 announce AS209847:AS-THE
import:          from AS44222 accept ANY
export:          to AS44222 announce AS209847:AS-THE
import:          from AS8285 accept ANY
export:          to AS8285 announce AS209847:AS-THE
import:          from AS15694 accept ANY
export:          to AS15694 announce AS209847:AS-THE
import:          from AS199081 accept ANY
export:          to AS199081 announce AS209847:AS-THE
```

Figure 15: *RIPE AS record for AS209847 (Source: RIPE DB)*

Maintainer Records and Links to Dmitrii Miasnikov

Insikt Group conducted further analysis on the email address *jama**[@]gmail[.]com*, which initially linked Stark Industries to UFO Hosting via RIPE database maintainer objects earlier in this report. This analysis revealed that the email address was not only associated with PQHS-MNT (PQ.Hosting maintainer) and UFO42-MNT (UFO Hosting maintainer), but also with the newly created THE-HOSTING-MNT. As of June 24, 2025, these maintainer objects were responsible for all of the new

RIPE organization objects outlined in this report, as well as further organizations tied to the Neculiti brothers, such as WEISS HOSTING GROUP S.R.L. (ORG-PHD16-RIPE; see **Figure 16**).

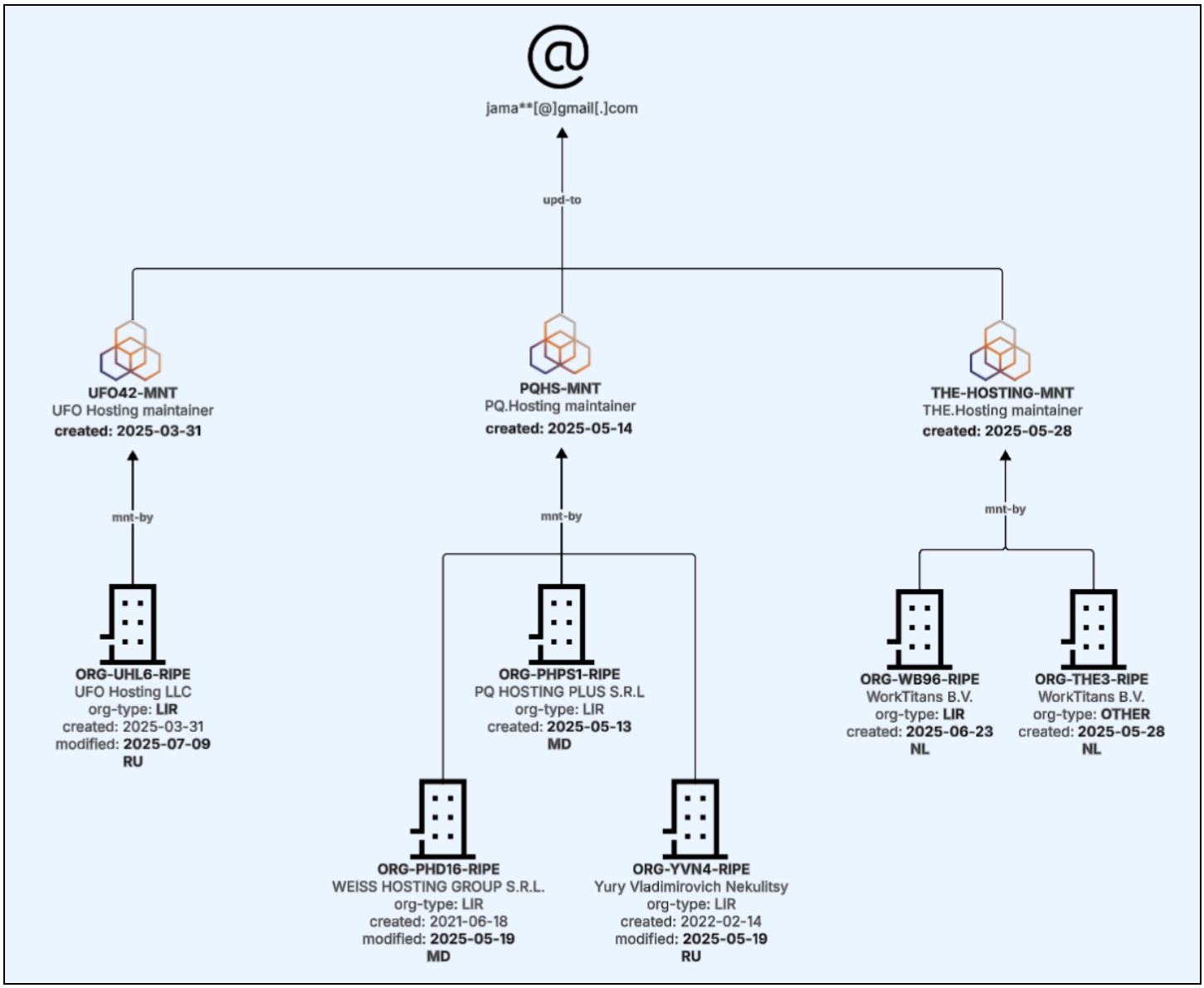

Figure 16: *Maintainer objects and organizations linked to email jama**[@]gmail[.]com (Source: Recorded Future / RIPE DB)*

Further research into this email address confirmed its attribution to Dmitrii Miasnikov, a known Russian network operator with prior affiliations to numerous Russia-based hosting providers. Specifically, the same email address was used to submit multiple RIPE NCC Executive Board nominations in April 2020 under Miasnikov's name, listing various Russian hosting entities as his affiliated organizations).

According to the RIPE database, Miasnikov also operates two LIRs under his own name, ORG-DAM5-RIPE and ORG-DAM6-RIPE. Insikt Group notes that as of June 24, 2025, only one prefix was assigned to ORG-DAM5-RIPE, *91[.]207[.]183[.]0/24*, which was outlined in **Appendix B**, as announced via AS33993 (UFO-AS).

Both objects contain the email address *admin[@]virty[.]io*, which refers to another Russian ISP, *virty[.]io*, which is owned by First Data Center LLC (ООО "Первый ЦОД"). In addition to traditional hosting, the company offers a number of what it calls "RIPE Object Support and Registration Services" (see **Figure 17**).

Figure 17: *Virty[.]io RIPE services web page (Source: virty[.]io)*

Insikt Group assesses that Miasnikov's control over RIPE object registration services, combined with his access to multiple LIRs and maintainer objects, likely enabled him to facilitate the creation, transfer, and operational handoff of RIPE assets for Stark Industries, allowing the sanctioned entity to sustain infrastructure continuity under new organizational entities.

Mitigations

- **Use Recorded Future Threat Intelligence:** Recorded Future customers can proactively mitigate threats originating from malicious networks such as Stark Industries by operationalizing Recorded Future Intelligence Cloud data, specifically by leveraging continuously updated Risk Lists and by blocklisting validated malicious IP addresses to prevent internal communication with malicious infrastructure.

- **Implement Robust Network Security Controls:** Configure perimeter security appliances and internal network defenses to block traffic originating from the ASNs identified in this report, unless there is a clearly defined business justification for permitting such traffic.

Outlook

Insikt Group assesses that Stark Industries will likely continue operating with minimal disruption under its new corporate entities, THE.Hosting and UFO Hosting, despite its inclusion in the EU's May 2025 sanctions package. The evidence outlined in this report demonstrates that the organization likely anticipated the EU sanctions and executed a deliberate, multi-phase restructuring of its hosting operations, using its parent company, PQ.Hosting, and Russian ISP, UFO Hosting.

While the EU sanctions did reference PQ.Hosting, the company's omission from a formal designation as part of the package, along with other linked entities, may have been a critical gap. This allowed Stark Industries to rapidly rebrand, transfer assets, and preserve operational control through affiliated RIPE organizations and front companies with relative ease.

Insikt Group will continue to monitor the infrastructure, affiliations, and evolution of this TAE network, as its persistent role in supporting global malicious cyber operations remains a critical indicator of future threat activity.

Appendix A: Malware Intelligence Queries

```
dynamic.network.ips.asn == "AS44477"
dynamic.network.ips.asn == "AS209847"
dynamic.network.ips.asn == "AS33993"
```

Appendix B: IP Prefixes Announced By AS33993 (UFO-AS)

Prefix	Organization	Country
2[.]56[.]178[.]0/24	UFO Hosting LLC	Russia
45[.]12[.]114[.]0/24	UFO Hosting LLC	Russia
45[.]12[.]115[.]0/24	UFO Hosting LLC	Russia
45[.]67[.]230[.]0/24	UFO Hosting LLC	Russia
45[.]84[.]1[.]0/24	UFO Hosting LLC	Russia
45[.]128[.]49[.]0/24	UFO Hosting LLC	Russia
45[.]128[.]53[.]0/24	UFO Hosting LLC	Russia
45[.]138[.]157[.]0/24	Stark Industries Solutions Ltd	Russia
45[.]144[.]30[.]0/24	UFO Hosting LLC	Russia
45[.]144[.]31[.]0/24	UFO Hosting LLC	Russia
45[.]150[.]64[.]0/24	UFO Hosting LLC	Russia
45[.]153[.]231[.]0/24	Stark Industries Solutions Ltd	Russia
91[.]207[.]183[.]0/24	Dmitrii Aleksandrovich Miasnikov	Russia
94[.]131[.]113[.]0/24	UFO Hosting LLC	Russia
94[.]131[.]121[.]0/24	UFO Hosting LLC	Russia
103[.]113[.]68[.]0/24	UFO Hosting LLC	Russia
171[.]22[.]119[.]0/24	UFO Hosting LLC	Russia
185[.]234[.]59[.]0/24	UFO Hosting LLC	Russia

Prefix	Organization	Country
185[.]235[.]242[.]0/24	UFO Hosting LLC	Russia
185[.]250[.]149[.]0/24	UFO Hosting LLC	Russia
193[.]201[.]126[.]0/24	Stark Industries Solutions Ltd	Russia

Appendix B: *IP Prefixes announced via AS33993, UFO-AS (Source: BGP.tools)*

Appendix C: IP Prefixes Announced By AS209847 (THE)

Prefix	Organization	Country
2[.]56[.]119[.]0/24	WorkTitans B.V	Latvia
5[.]182[.]39[.]0/24	WorkTitans B.V	Portugal
45[.]12[.]131[.]0/24	WorkTitans B.V	Portugal
45[.]15[.]178[.]0/24	WorkTitans B.V	Bosnia and Herzegovina
45[.]15[.]179[.]0/24	WorkTitans B.V	Bosnia and Herzegovina
45[.]15[.]184[.]0/24	WorkTitans B.V	Bosnia and Herzegovina
45[.]83[.]142[.]0/24	WorkTitans B.V	Portugal
45[.]133[.]216[.]0/24	-	Latvia
45[.]142[.]213[.]0/24	-	Latvia
45[.]142[.]215[.]0/24	-	Latvia
45[.]159[.]251[.]0/24	WorkTitans B.V	Portugal
94[.]131[.]10[.]0/24	WorkTitans B.V	Portugal
94[.]131[.]104[.]0/24	WorkTitans B.V	Latvia
95[.]164[.]32[.]0/24	WorkTitans B.V	Portugal
103[.]231[.]73[.]0/24	WorkTitans B.V	Latvia
171[.]22[.]129[.]0/24	WorkTitans B.V	Portugal
176[.]120[.]67[.]0/24	WorkTitans B.V	Latvia

Prefix	Organization	Country
193[.]43[.]146[.]0/24	WorkTitans B.V	Latvia
2a09:7c43::/32	WorkTitans B.V	Latvia
2a0b:cf43::/32	WorkTitans B.V	Portugal
2a0b:cf43::/32	WorkTitans B.V	Bosnia and Herzegovina

Appendix C: *IP prefixes announced via AS209847, THE (Source: BGP.tools)*

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com