

Stark Industries Solutions: An Iron Hammer in the Cloud

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

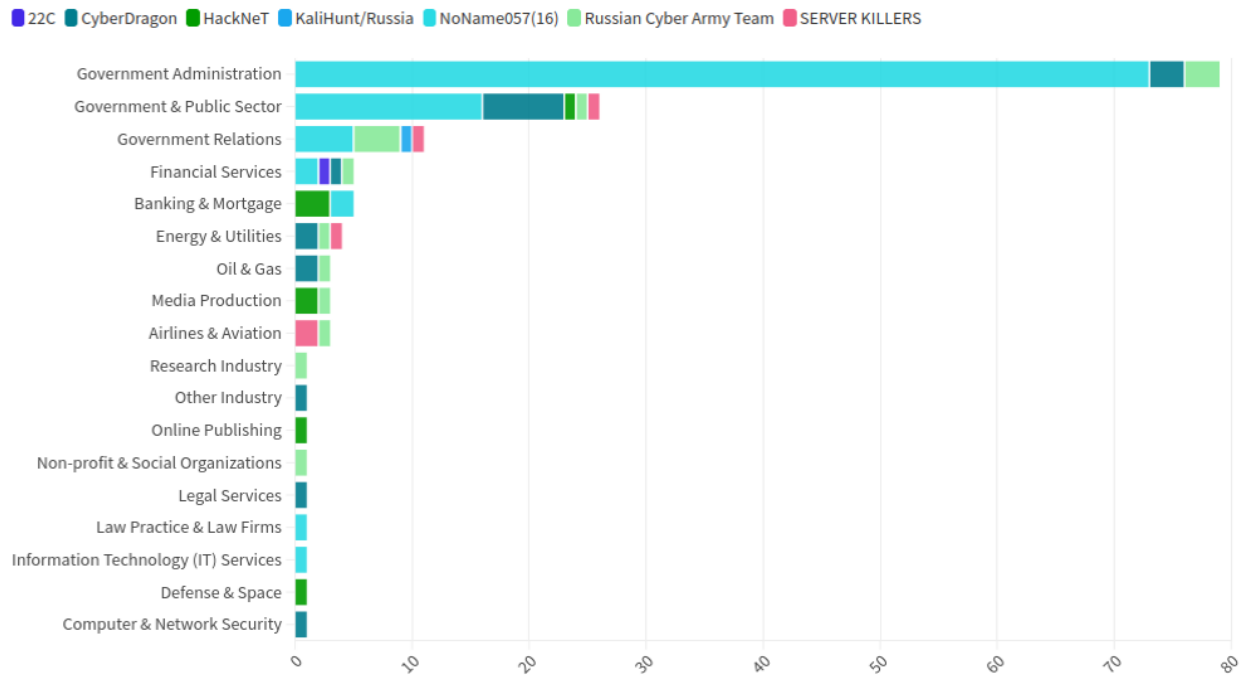


The homepage of Stark Industries Solutions.

Two weeks before Russia invaded Ukraine in February 2022, a large, mysterious new Internet hosting firm called **Stark Industries Solutions** materialized and quickly became the epicenter of massive distributed denial-of-service (DDoS) attacks on government and commercial targets in Ukraine and Europe. An investigation into Stark Industries reveals it is being used as a global proxy network that conceals the true source of cyberattacks and disinformation campaigns against enemies of Russia.

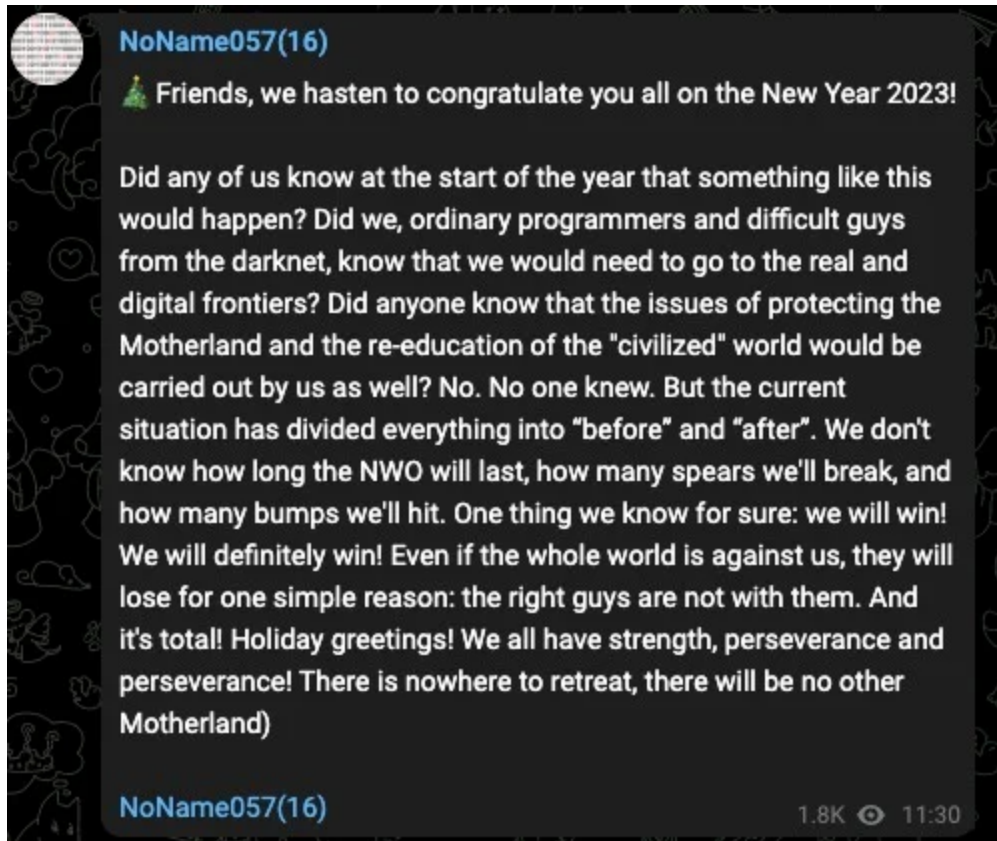
At least a dozen patriotic Russian hacking groups have been launching DDoS attacks since the start of the war at a variety of targets seen as opposed to Moscow. But by all accounts, few attacks from those gangs have come close to the amount of firepower wielded by a pro-Russia group calling itself “**NoName057(16)**.”

Hacktivist DDoS Attack Claims (March to May 2024)



This graphic comes from a recent report from NETSCOUT about DDoS attacks from Russian hacktivist groups.

As detailed by researchers at [Radware](#), NoName has effectively gamified DDoS attacks, recruiting hacktivists via its Telegram channel and offering to pay people who agree to install a piece of software called **DDoSia**. That program allows NoName to commandeer the host computers and their Internet connections in coordinated DDoS campaigns, and DDoSia users with the most attacks can win cash prizes.



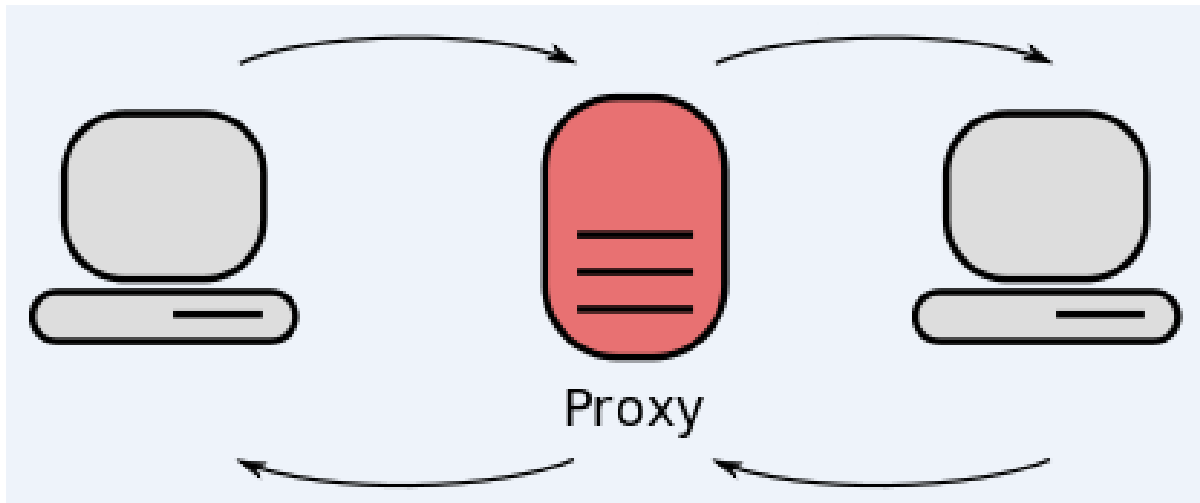
The NoName DDoS group advertising on Telegram. Image: SentinelOne.com.

A [report](#) from the security firm **Team Cymru** found the DDoS attack infrastructure used in NoName campaigns is assigned to two interlinked hosting providers: **MIRhosting** and **Stark Industries**. MIRhosting is a hosting provider founded in The Netherlands in 2004. But [Stark Industries Solutions Ltd](#) was incorporated on February 10, 2022, just two weeks before the Russian invasion of Ukraine.

PROXY WARS

Security experts say that not long after the war started, Stark began hosting dozens of proxy services and free virtual private networking (VPN) services, which are designed to help users shield their Internet usage and location from prying eyes.

Proxy providers allow users to route their Internet and Web browsing traffic through someone else's computer. From a website's perspective, the traffic from a proxy network user appears to originate from the rented IP address, not from the proxy service customer.



These services can be used in a legitimate manner for several business purposes — such as price comparisons or sales intelligence — but they are also massively abused for hiding cybercrime activity because they can make it difficult to trace malicious traffic to its original source.

What's more, many proxy services do not disclose how they obtain access to the proxies they are renting out, and in many cases the access is obtained through the dissemination of malicious software that turns the infected system into a traffic relay — usually unbeknownst to the legitimate owner of the Internet connection. Other proxy services will allow users to make money by renting out their Internet connection to anyone.

Spur.us is a company that tracks VPNs and proxy services worldwide. Spur finds that Stark Industries (AS44477) currently is home to at least 74 VPN services, and 40 different proxy services. As we'll see in the final section of this story, just one of those proxy networks has over a million Internet addresses available for rent across the globe.

Raymond Dijkhoorn operates a hosting firm in The Netherlands called Prolocation. He also co-runs SURBL, an anti-abuse service that flags domains and Internet address ranges that are strongly associated with spam and cybercrime activity, including DDoS.

Dijkhoorn said last year SURBL heard from multiple people who said they operated VPN services whose web resources were included in SURBL's block lists.

"We had people doing delistings at SURBL for domain names that were suspended by the registrars," Dijkhoorn told KrebsOnSecurity. "And at least two of them explained that Stark offered them free VPN services that they were reselling."

Dijkhoorn added that Stark Industries also sponsored activist groups from Ukraine.

"How valuable would it be for Russia to know the real IPs from Ukraine's tech warriors?" he observed.

LOUDY WITH A CHANCE OF BULLETS

Richard Hummel is threat intelligence lead at **NETSCOUT**. Hummel said when he considers the worst of all the hosting providers out there today, Stark Industries is consistently near or at the top of that list.

“The reason is we’ve had at least a dozen service providers come to us saying, ‘There’s this network out there inundating us with traffic,’” Hummel said. “And it wasn’t even DDoS attacks. [The systems] on Stark were just scanning these providers so fast it was crashing some of their services.”

Hummel said NoName will typically launch their attacks using a mix of resources rented from major, legitimate cloud services, and those from so-called “**bulletproof**” hosting providers like Stark. Bulletproof providers are so named when they earn or cultivate a reputation for ignoring any abuse complaints or police reports about activity on their networks.

Combining bulletproof providers with legitimate cloud hosting, Hummel said, likely makes NoName’s DDoS campaigns more resilient because many network operators will hesitate to be too aggressive in blocking Internet addresses associated with the major cloud services.

“What we typically see here is a distribution of cloud hosting providers and bulletproof hosting providers in DDoS attacks,” he said. “They’re using public cloud hosting providers because a lot of times that’s your first layer of network defense, and because [many companies are wary of] over-blocking access to legitimate cloud resources.”

But even if the cloud provider detects abuse coming from the customer, the provider is probably not going to shut the customer down immediately, Hummel said.

“There is usually a grace period, and even if that’s only an hour or two, you can still launch a large number of attacks in that time,” he said. “And then they just keep coming back and opening new cloud accounts.”

MERCENARIES TEAM

Stark Industries is incorporated at a mail drop address in the United Kingdom. UK business records list an **Ivan Vladimirovich Neculiti** as the company’s secretary. Mr. Neculiti also is named as the CEO and founder of **PQ Hosting Plus S.R.L.** (aka Perfect Quality Hosting), a Moldovan company formed in 2019 that lists the same UK mail drop address as Stark Industries.

Reached via LinkedIn, Mr. Neculiti said PQ Hosting established Stark Industries as a “white label” of its brand so that “resellers could distribute our services using our IP addresses and their clients would not have any affairs with PQ Hosting.”

“PQ Hosting is a company with over 1,000+ of [our] own physical servers in 38 countries and we have over 100,000 clients,” he said. “Though we are not as large as Hetzner, Amazon and OVH, nevertheless we are a fast growing company that provides services to tens of thousands of private customers and legal entities.”

Asked about the constant stream of DDoS attacks whose origins have traced back to Stark Industries over the past two years, Neculiti maintained Stark hasn’t received any official abuse reports about attacks coming from its networks.



Ivan Neculiti, as pictured on LinkedIn.

“It was probably some kind of clever attack that we did not see, I do not rule out this fact, because we have a very large number of clients and our Internet channels are quite large,” he said. “But, in this situation, unfortunately, no one contacted us to report that there was an attack from our addresses; if someone had contacted us, we would have definitely blocked the network data.”

DomainTools.com finds Ivan V. Neculiti was the owner of **war[.]md**, a website launched in 2008 that chronicled the history of a 1990 armed conflict in Moldova known as the Transnistria War and the Moldo-Russian war.



An ad for war.md, circa 2009.

Transnistria is a breakaway pro-Russian region that declared itself a state in 1990, although it is not internationally recognized. The copyright on that website credits the “**MercenarieS TeaM**,” which was at one time a Moldovan IT firm. Mr. Neculiti confirmed personally registering this domain.

DON CHICHO & DFYZ

The data breach tracking service Constella Intelligence reports that an Ivan V. Neculiti registered multiple online accounts under the email address **dfyz_bk@bk.ru**. Cyber intelligence firm Intel 471 shows this email address is tied to the username “**dfyz**” on more than a half-dozen Russian language cybercrime forums since 2008. The user dfyz on Searchengines[.]ru in 2008 asked other forum members to review war.md, and said they were part of the MercenarieS TeaM.

Back then, dfyz was selling “bulletproof servers for any purpose,” meaning the hosting company would willfully ignore abuse complaints or police inquiries about the activity of its customers.

DomainTools reports there are at least 33 domain names registered to dfyz_bk@bk.ru. Several of these domains have Ivan Neculiti in their registration records, including tracker-free[.]cn, which was registered to an Ivan Neculiti at dfyz_bk@bk.ru and referenced the Mercenaries TeaM in its original registration records.

Dfyz also used the nickname **DonChicho**, who likewise sold bulletproof hosting services and access to hacked Internet servers. In 2014, a prominent member of the Russian language cybercrime community **Antichat** filed a complaint against DonChicho, saying this user scammed them and had used the email address dfyz_bk@bk.ru.

The complaint said DonChicho registered on Antichat from the Transnistria Internet address **84.234.55[.]29**. Searching this address in Constella reveals it has been used to register just five accounts online that have been created over the years, including one at ask.ru, where the user registered with the email address **neculity1@yandex.ru**. Constella also returns for that email address a user by the name “Ivan” at memoraleak.com and 000webhost.com.

Constella finds that the password most frequently used by the email address dfyz_bk@bk.ru was “**filecast**,” and that there are more than 90 email addresses associated with this password. Among them are roughly two dozen addresses with the name “Neculiti” in them, as well as the address **support@donservers[.]ru**.

Intel 471 says DonChicho posted to several Russian cybercrime forums that support@donservers[.]ru was his address, and that he logged into cybercrime forums almost exclusively from Internet addresses in Tiraspol, the capital of Transnistria. A review of DonChicho’s posts shows this person was banned from several forums in 2014 for scamming other users.

Cached copies of DonChicho’s vanity domain ([donchicho\[.\]ru](http://donchicho[.]ru)) show that in 2009 he was a spammer who peddled knockoff prescription drugs via Rx-Promotion, once one of the largest pharmacy spam moneymaking programs for Russian-speaking affiliates.

Mr. Neculiti told KrebsOnSecurity he has never used the nickname DonChicho.

“I may assure you that I have no relation to DonChicho nor to his bulletproof servers,” he said.

Below is a mind map that shows the connections between the accounts mentioned above.

A mind map tracing the history of the user Dfyz. Click to enlarge.

Earlier this year, NoName began massively hitting government and industry websites in Moldova. A [new report](#) from **Arbor Networks** says the attacks began around March 6, when NoName alleged the government of Moldova was “craving for Russophobia.”

“Since early March, more than 50 websites have been targeted, according to posted ‘proof’ by the groups involved in attacking the country,” Arbor’s **ASERT Team** [wrote](#). “While NoName seemingly initiated the ramp of attacks, a host of other DDoS hacktivists have joined the fray in claiming credit for attacks across more than 15 industries.”

CORRECTIV ACTION

The German independent news outlet **Correctiv.org** last week published a [scathing investigative report on Stark Industries and MIRhosting](#), which notes that Ivan Neculiti operates his hosting companies [with the help of his brother, Yuri](#).

The report points out that Stark Industries continues to host a Russian disinformation news outlet called “Recent Reliable News” (RRN) that was [sanctioned by the European Union in 2023](#) for spreading links to propaganda blogs and fake European media and government websites.

“The website was not running on computers in Moscow or St. Petersburg until recently, but in the middle of the EU, in the Netherlands, on the computers of the Neculiti brothers,” Correctiv reporters wrote.

“After a request from this editorial team, a well-known service was installed that hides the actual web host,” the report continues. “Ivan Neculiti announced that he had blocked the associated access and server following internal investigations. “We very much regret that we are only now finding out that one of our customers is a sanctioned portal,” said the company boss. However, RRN is still accessible via its servers.”

Correctiv also points to a January 2023 report from the Ukrainian government, which found servers from Stark Industries Solutions were used as part of a cyber attack on the Ukrainian news agency “**Ukrinform**”. Correctiv notes the notorious hacker group Sandworm — an advanced persistent threat (APT) group operated by a cyberwarfare unit of Russia’s military intelligence service — was identified by Ukrainian government authorities as responsible for that attack.

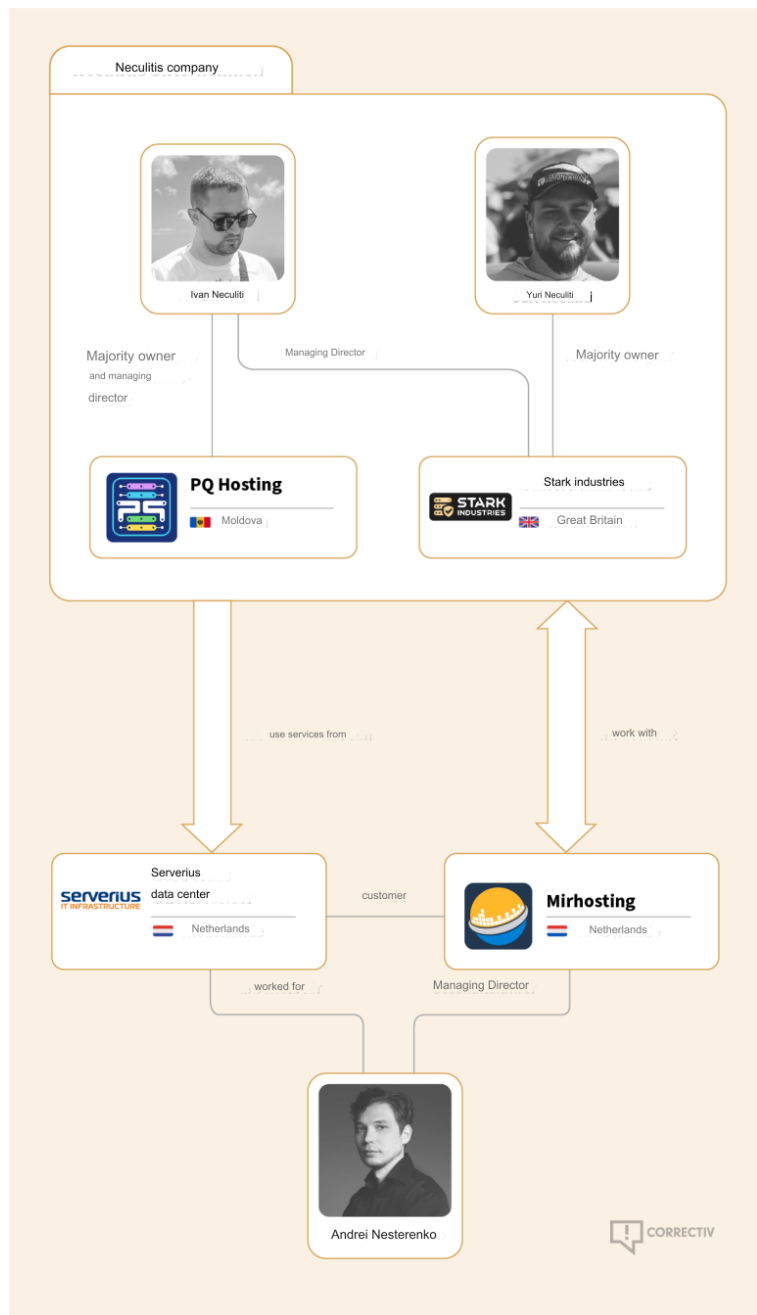


Image credit: correctiv.org.

PEACE HOSTING?

Public records indicate MIRhosting is based in The Netherlands and is operated by 37-year old **Andrey Nesterenko**, whose personal website says he is an accomplished concert pianist who began performing publicly at a young age.

DomainTools says mirhosting[.]com is registered to Mr. Nesterenko and to **Innovation IT Solutions Corp**, which lists addresses in London and in Nesterenko’s stated hometown of Nizhny Novgorod, Russia.

This is interesting because according to the book *Inside Cyber Warfare* by **Jeffrey Carr**, Innovation IT Solutions Corp. was responsible for hosting **StopGeorgia[.]ru**, a hacktivist website for organizing cyberattacks against Georgia that appeared at the same time Russian forces invaded the former Soviet nation in 2008. That conflict was thought to be the first war ever fought in which a notable cyberattack and an actual military engagement happened simultaneously.

Responding to questions from KrebsOnSecurity, Mr. Nesterenko said he couldn't say whether his network had ever hosted the StopGeorgia website back in 2008 because his company didn't keep records going back that far. But he said Stark Industries Solutions is indeed one of MIRhosting's colocation customers.

"Our relationship is purely provider-customer," Nesterenko said. "They also utilize multiple providers and data centers globally, so connecting them directly to MIRhosting overlooks their broader network."

"We take any report of malicious activity seriously and are always open to information that can help us identify and prevent misuse of our infrastructure, whether involving Stark Industries or any other customer," Nesterenko continued. "In cases where our services are exploited for malicious purposes, we collaborate fully with Dutch cyber police and other relevant authorities to investigate and take appropriate measures. However, we have yet to receive any actionable information beyond the article itself, which has not provided us with sufficient detail to identify or block malicious actors."

In December 2022, security firm Recorded Future profiled the phishing and credential harvesting infrastructure used for Russia-aligned espionage operations by a group dubbed **Blue Charlie** (aka **TAG-53**), which has targeted email accounts of nongovernmental organizations and think tanks, journalists, and government and defense officials.

Recorded Future found that virtually all the Blue Charlie domains existed in just ten different ISPs, with a significant concentration located in two networks, one of which was MIRhosting. Both Microsoft and the UK government assess that Blue Charlie is linked to the Russian threat activity groups variously known as **Callisto Group**, **COLDRIVER**, and **SEABORGIUM**.

Mr. Nesterenko took exception to a story on that report from *The Record*, which is owned by Recorded Future.

"We've discussed its contents with our customer, Stark Industries," he said. "We understand that they have initiated legal proceedings against the website in question, as they firmly believe that the claims made are inaccurate."

Recorded Future said they updated their story with comments from Mr. Neculiti, but that they stand by their reporting.

Mr. Nesterenko's LinkedIn profile says he was previously the foreign region sales manager at **Serverius-as**, a hosting company in The Netherlands that remains in the same data center as MIRhosting.

In February, the Dutch police took 13 servers offline that were used by the infamous LockBit ransomware group, which had originally bragged on its darknet website that its home base was in The Netherlands. Sources tell KrebsOnSecurity the servers seized by the Dutch police were located in Serverius' data center in Dronten, which is also shared by MIRhosting.

Serverius-as did not respond to requests for comment. Nesterenko said MIRhosting does use one of Serverius's data centers for its operations in the Netherlands, alongside two other data centers, but that the recent incident involving the seizure of servers has no connection to MIRhosting.

"We are legally prohibited by Dutch law and police regulations from sharing information with third parties regarding any communications we may have had," he said.

A February 2024 report from security firm **ESET** found Serverius-as systems were involved in a series of targeted phishing attacks by Russia-aligned groups against Ukrainian entities throughout 2023. ESET observed that after the spearphishing domains were no longer active, they were converted to promoting rogue Internet pharmacy websites.

PEERING INTO THE VOID

A review of the Internet address ranges recently added to the network operated by Stark Industries Solutions offers some insight into its customer base, usage, and maybe even true origins. Here is a snapshot (PDF) of all Internet address ranges announced by Stark Industries so far in the month of May 2024 (this information was graciously collated by the network observability platform Kentik.com).

Those records indicate that the largest portion of the IP space used by Stark is in The Netherlands, followed by Germany and the United States. Stark says it is connected to roughly 4,600 Internet addresses that currently list their ownership as **Comcast Cable Communications**.

A review of those address ranges at spur.us shows all of them are connected to an entity called **Proxyline**, which is a sprawling proxy service based in Russia that currently says it has more than 1.6 million proxies globally that are available for rent.

The screenshot shows the ProxyLine website catalog page. The header includes the site name 'ProxyLine' with the tagline 'СТАБИЛЬНОСТЬ И КОМФОРТ' and navigation links for 'PROXY SERVERS', 'IPV4', 'IPV6', 'PRICES', 'AFFILIATE PROGRAM', 'PROXY WHOLESALE', and 'CONTACTS'. There are also buttons for 'Authorization', 'Registration', and a language selector for 'RU'. A secondary navigation bar contains icons for 'PROXY CHECKER', 'SPEED', 'PORTS', 'MY IP', 'ANONYMITY', 'BLACK LIST', 'IPV6', 'API', and 'FREE PROXIES'. The main content area is titled 'PROXY SERVERS' and features three product cards:

- IPv4 Shared PROXY**: Used by up to 3 people. Country: Australia. Qty: 1. Price per piece: 0.67\$ (~60.90 P). Period: 5 days.
- Individual IPv4 PROXIES**: Issued in one hand. Country: Russia, Russia). Qty: 1. Price per piece: 0.97\$ (~88.16 P). Period: 5 days.
- IPv6/32 PROXY**: Issued in one hand. Country: United States. Qty: 1. Price per piece: 0.1\$ (~9.09 P). Period: 5 days.

Additional elements include a 'BUY WITH' badge with cryptocurrency icons, a 'ПОПУЛЯРНЫЙ ВЫБОР' (Popular Choice) badge with social media icons, and a 'ГАРАНТИЯ ВОЗВРАТ ИЛИ ЗАМЕНА IP 48 ЧАСОВ' (48-hour IP return or replacement guarantee) star badge.

Reached for comment, Comcast said the Internet address ranges never did belong to Comcast, so it is likely that Stark has been fudging the real location of its routing announcements in some cases.

Stark reports that it has more than 67,000 Internet addresses at Santa Clara, Calif.-based **EGIhosting**. Spur says the Stark addresses involving EGIhosting all map to Proxyline as well. EGIhosting did not respond to requests for comment.

EGIhosting manages Internet addresses for the Cyprus-based hosting firm **ITHOSTLINE LTD** (aka **HOSTLINE-LTD**), which is represented throughout Stark's announced Internet ranges. Stark says it has more than 21,000 Internet addresses with HOSTLINE. Spur.us finds Proxyline addresses are especially concentrated in the Stark ranges labeled ITHOSTLINE LTD, HOSTLINE-LTD, and **Proline IT**.

Stark's network list includes approximately 21,000 Internet addresses at Hockessin, De. based **DediPath**, which abruptly ceased operations without warning in August 2023. According to a phishing report released last year by **Interisle Consulting**, DediPath was the fourth most common source of phishing attacks in the year ending Oct. 2022. Spur.us likewise finds that virtually all of the Stark address ranges marked "DediPath LLC" are tied to Proxyline.

Case Study #2: DEDIPATH

Like A2HOSTING, [DEDIPATH](#) offers a number of hosting services. We observed a huge uptick in phishing attacks reported at [DEDIPATH](#) during the August 2022 – October 2022 period. [DEDIPATH](#) typically had very few IPv4 addresses reported for hosting phishing, but phishing attacks launched using the from accounts created at the subdomain service provider, DUCKDNS.ORG vaulted [DEDIPATH](#) into our “phishiest” hosting networks in our 2023 study.



Image: Interisle Consulting.

A large number of the Internet address ranges announced by Stark in May originate in India, and the names that are self-assigned to many of these networks indicate they were previously used to send large volumes of spam for herbal medicinal products, with names like **HerbalFarm**, **AdsChrome**, **Nutravo**, **Herbzoot** and **Herbalve**.

The anti-spam organization **SpamHaus** [reports](#) that many of the Indian IP address ranges are associated with known “snowshoe spam,” a form of abuse that involves mass email campaigns spread across several domains and IP addresses to weaken reputation metrics and avoid spam filters.

It’s not clear how much of Stark’s network address space traces its origins to Russia, but big chunks of it recently belonged to some of the oldest entities on the Russian Internet (a.k.a. “Runet”).

For example, many Stark address ranges were most recently assigned to a Russian government entity whose full name is the “**Federal State Autonomous Educational Establishment of Additional Professional Education Center of Realization of State Educational Policy and Informational Technologies.**”

A review of [Internet address ranges adjacent to this entity](#) reveals a long list of Russian government organizations that are part of the **Federal Guard Service of the Russian Federation**. [Wikipedia says](#) the Federal Guard Service is a Russian federal government agency concerned with tasks related to protection of several high-ranking state officials, including the President of Russia, as well as certain federal properties. The agency traces its origins to the USSR’s Ninth Directorate of the KGB, and later the presidential security service.

Stark recently announced the address range 213.159.64.0/20 from April 27 to May 1, and this range was previously assigned to an ancient ISP in St. Petersburg, RU called the **Computer Technologies Institute Ltd.**

According to a post on the Russian language webmaster forum searchengines[.]ru, the domain for Computer Technologies Institute — **ctinet[.]ru** — *is the seventh-oldest domain in the entire history of the Runet.*

Curiously, Stark also lists large tracts of Internet addresses (close to 48,000 in total) assigned to a small ISP in Kharkiv, Ukraine called **NetAssist**. Reached via email, the CEO of NetAssist **Max Tulyev** confirmed his company provides a number of services to PQ Hosting.

“We colocate their equipment in Warsaw, Madrid, Sofia and Thessaloniki, provide them IP transit and IPv4 addresses,” Tulyev said. “For their size, we receive relatively low number of complains to their networks. I never seen anything about their pro-Russian activity or support of Russian hackers. It is very interesting for me to see proofs of your accusations.”

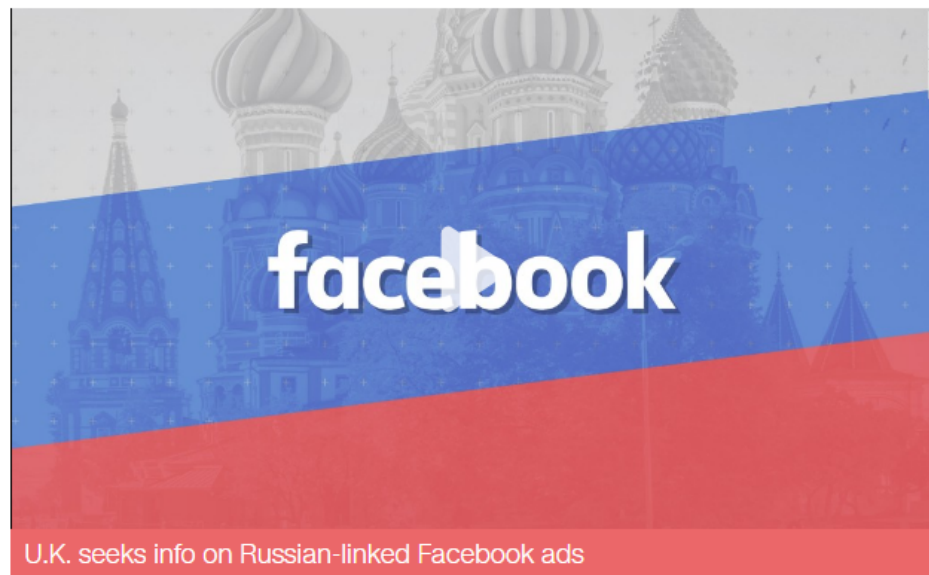
Spur.us mapped the entire infrastructure of Proxyline, and found more than one million proxies across multiple providers, but by far the biggest concentration was at Stark Industries Solutions. The [full list of Proxyline address ranges](#) (.CSV) shows two other ISPs appear repeatedly throughout the list. One is Kharkiv, Ukraine based **ITL LLC**, also known as **Information Technology Laboratories Group**, and **Integrated Technologies Laboratory**.

The second is a related hosting company in Miami, called **Green Floid LLC**. Green Floid featured in [a 2017 scoop by CNN](#), which profiled the company’s owner and quizzed him about Russian troll farms using proxy networks on Green Floid and its parent firm ITL to mask disinformation efforts tied to the Kremlin’s [Internet Research Agency](#) (IRA). At the time, the IRA was using Facebook and other social media networks to spread videos showing police brutality against African Americans in an effort to encourage protests across the United States.

From Silicon Valley to Staten Island, Russian troll sites kept online by American companies

by Jose Pagliery and Donie O'Sullivan @CNMoney

🕒 October 25, 2017: 8:12 AM ET



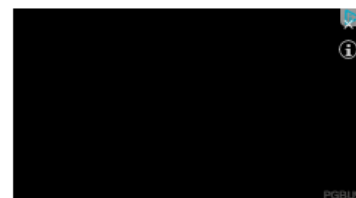
Newsletter

RELIABLE SOURCES

Brian Stelter's must-read media newsletter

[Click to subscribe >](#)

Recommended by Outbrain



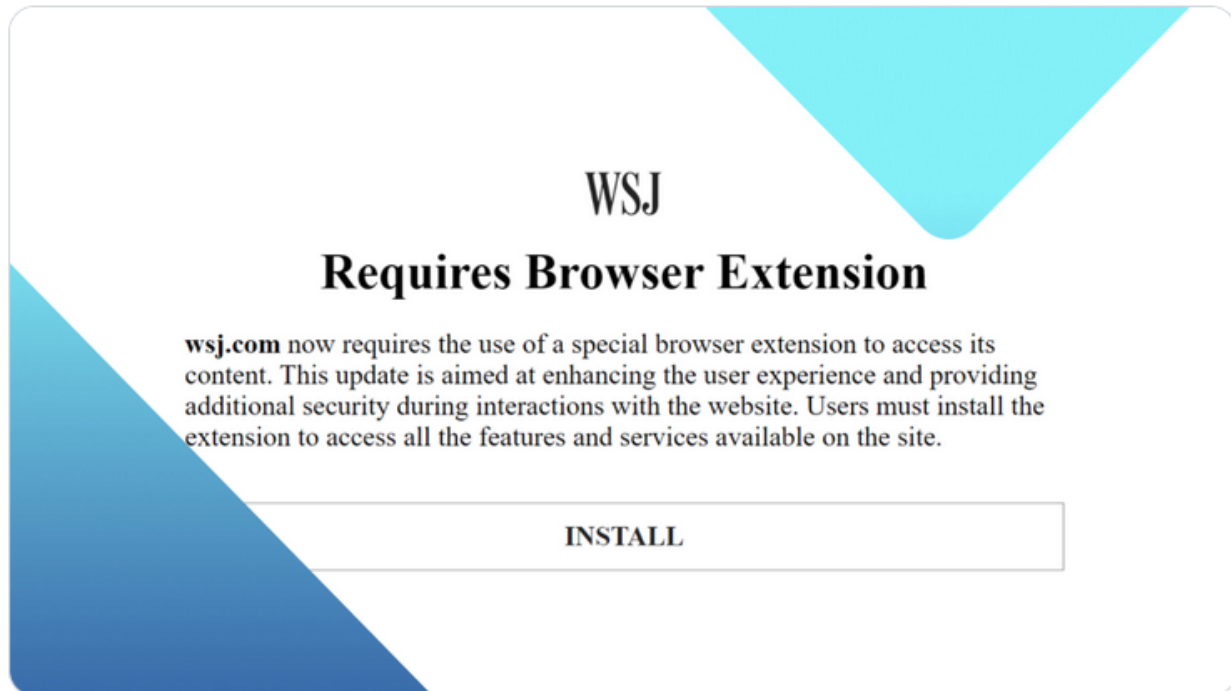
The use of American companies to push Russian propaganda goes beyond social media sites like Facebook. Russians also used American internet services to keep their websites up and hide their true owners, according to internet records and two executives at internet routing companies interviewed by CNN.

Doug Madory, director of Internet analysis at Kentik, was able to see at a high level the top sources and destinations for traffic traversing Stark's network.

"Based on our aggregate NetFlow, we see Iran as the top destination (35.1%) for traffic emanating from Stark (AS44477)," Madory said. "Specifically, the top destination is MTN Irancell, while the top source is Facebook. This data supports the theory that AS44477 houses proxy services as Facebook is blocked in Iran."

On April 30, the security firm **Malwarebytes** explored an extensive malware operation that targets corporate Internet users with malicious ads. Among the sites used as lures in that campaign were fake **Wall Street Journal** and CNN websites that told visitors they were required to install a WSJ or CNN-branded browser extension (malware). Malwarebytes found a domain name central to that operation was hosted at Internet addresses owned by Stark Industries.

[Home](#) > [Blog](#)



WSJ

Requires Browser Extension

wsj.com now requires the use of a special browser extension to access its content. This update is aimed at enhancing the user experience and providing additional security during interactions with the website. Users must install the extension to access all the features and services available on the site.

[INSTALL](#)

THREAT INTELLIGENCE

Corporate users targeted via malicious ads and modals

Posted: April 30, 2024 by [Jerome Segura](#)

Image: threatdown.com