ActiveFence

A Rising Star in Russia's Disinformation Game

The Beregini Hacking Group

March 3, 2022

Contents

Executive Summary

As tensions escalate in Ukraine, technology companies are taking dramatic steps to decreasing the spread of disinformation on their platforms. However, as platforms utilize more advanced measures, disinformation actors –specifically the Russian government – are becoming progressively sophisticated in their dissemination tactics. Seeking to keep this disinformation off their platforms, technology companies should be monitoring both official and unofficial state accounts, and identifying disinformation narratives in their infancy.

The following report will provide an overview of the Beregini group, a previously little-known group that appears to act on behalf of the Russian government. A self-described, ostensibly Ukrainian "hack and leak" group, Beregini disseminates seemingly official documents that support Russian propaganda.

Understanding the Beregini Group and the narratives they support, will allow technology companies to identify their activities, as they reach their platform in order to take action.

- The Beregini group claims to be Ukrainian and operates in Russian. The group leaks documents that support Russian narratives.
- Active since 2016, the group's content gained little attention before February, 2022, when it began leaking documents that support the increasingly belligerent Russian claims in the buildup to the current war.
- Mostly active on Telegram, the group's obscurity has allowed its content to be shared across the web, including major social platforms.
- The objectives of these attacks appear to be to sow discord in Ukraine, present the Ukrainian military as inept and weak, portray Ukraine as a puppet of Western regimes against Russia, and shift the blame of psychological warfare to Ukraine.

The Changing Face of Disinformation

In recent years, technology companies seeking to maintain the authenticity of their platforms and avoid being weaponized, have implemented advanced measures to keep disinformation and other online harms at bay.

However, as platforms take a greater stance against these activities, disinformation actors become more sophisticated in the measures they take to spread their harmful narratives. These include utilizing a wide range of affiliated, and what appear to be unaffiliated agents to access, manipulate, and spread content across all online platforms - large and small.

Russia's Information Warfare

Having established one of the most advanced disinformation engines in the world, Russia has spent years spreading false narratives that support its information warfare against international opponents, as well as sway the opinion of its own populace in support of government actions. Over time, Russia has established and maintained a vast network of official State media outlets as well as unofficial agents including websites, journalists, "think tanks" and political activists, that aid its disinformation war.

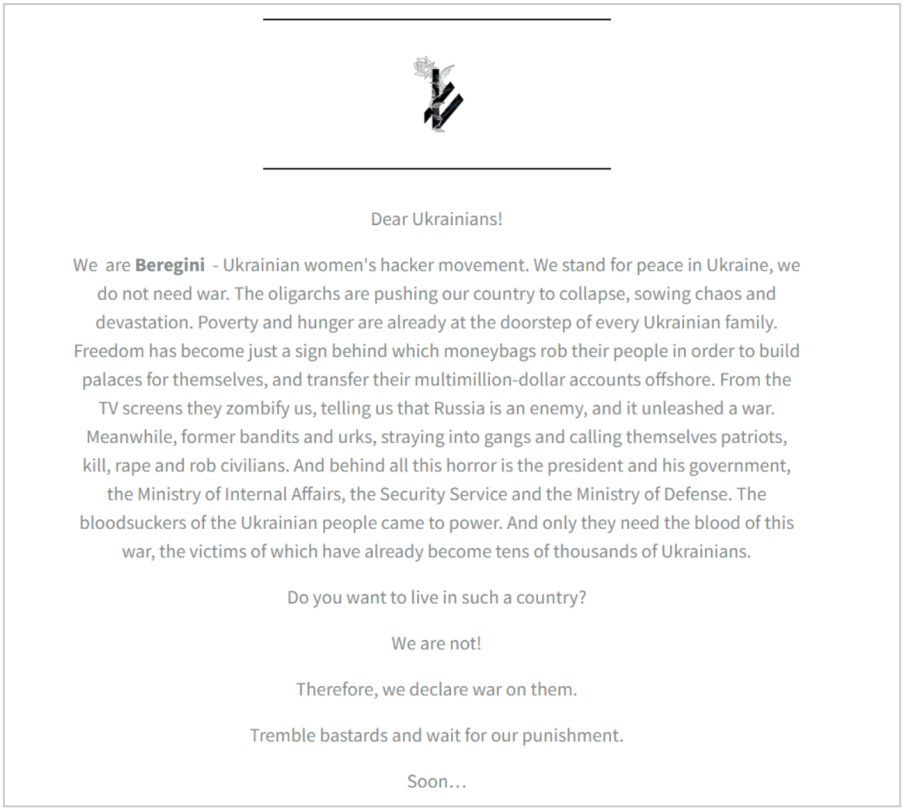
In the face of recent tensions, platforms have taken a more active stance against Russian disinformation, pushing the Kremlin to utilize more sophisticated methods, involving what appear to be unaffiliated entities to both spread disinformation, and allegedly hack and leak sensitive government documents. These tactics are used to support the Russian narrative of a strong Russian military and a weak adversary, while gaining public support for the war.

This report will provide an analysis of a group engaging in these activities.

The Beregini Hacking Group: a Rising Star in Russia's Disinformation Game

Acting covertly since 2016, the Beregini Group appears to be a hacking group working in the service or support of the Russian State. Communicating in Russian, the group claims to be a Ukrainian female hacking group acting in the best interest of the Ukrainian people, promoting peace, and opposing the Ukrainian government. The group's activities have only been covered in biased, pro-Russian media sources, supporting the notion that they are indeed a Russian group.

The group has collaborated at least once with Sprut, and an EU report claims that Beregini, Sprut, and Sandworm may have worked "in tandem" in the past. Their preferred mode of operation involves "Hack and Leak" attacks - which involve the dissemination of sensitive documents that have allegedly been hacked by the group. The group also engages in doxxing attacks - sharing sensitive personal information of Ukrainian officials and soldiers.



Dear Ukrainians!

We are **Beregini** - Ukrainian women's hacker movement. We stand for peace in Ukraine, we do not need war. The oligarchs are pushing our country to collapse, sowing chaos and devastation. Poverty and hunger are already at the doorstep of every Ukrainian family. Freedom has become just a sign behind which moneybags rob their people in order to build palaces for themselves, and transfer their multimillion-dollar accounts offshore. From the TV screens they zombify us, telling us that Russia is an enemy, and it unleashed a war. Meanwhile, former bandits and urks, straying into gangs and calling themselves patriots, kill, rape and rob civilians. And behind all this horror is the president and his government, the Ministry of Internal Affairs, the Security Service and the Ministry of Defense. The bloodsuckers of the Ukrainian people came to power. And only they need the blood of this war, the victims of which have already become tens of thousands of Ukrainians.

Do you want to live in such a country?

We are not!

Therefore, we declare war on them.

Tremble bastards and wait for our punishment.

Soon…

Image taken from the "About" section of Beregini's website

Previous Attacks

In recent years, the Beregini Group has leaked numerous Ukrainian military documents and made various claims about the Ukrainian government and related entities. These include:

- Leaks of various military forms and documents
- Alleged claims of Ukrainian war crimes
- Claims of COVID-19 vaccine inefficacy and lack of vaccine popularity in the Ukrainian military
- Doxxing Ukrainian defense officials
- Documents and statistics about Ukrainian training exercises abroad
- Claims of Ukrainian support for ISIS
- Claims of Ukrainian involvement in information warfare, using social media and bots against Russia.

Utilizing Telegram

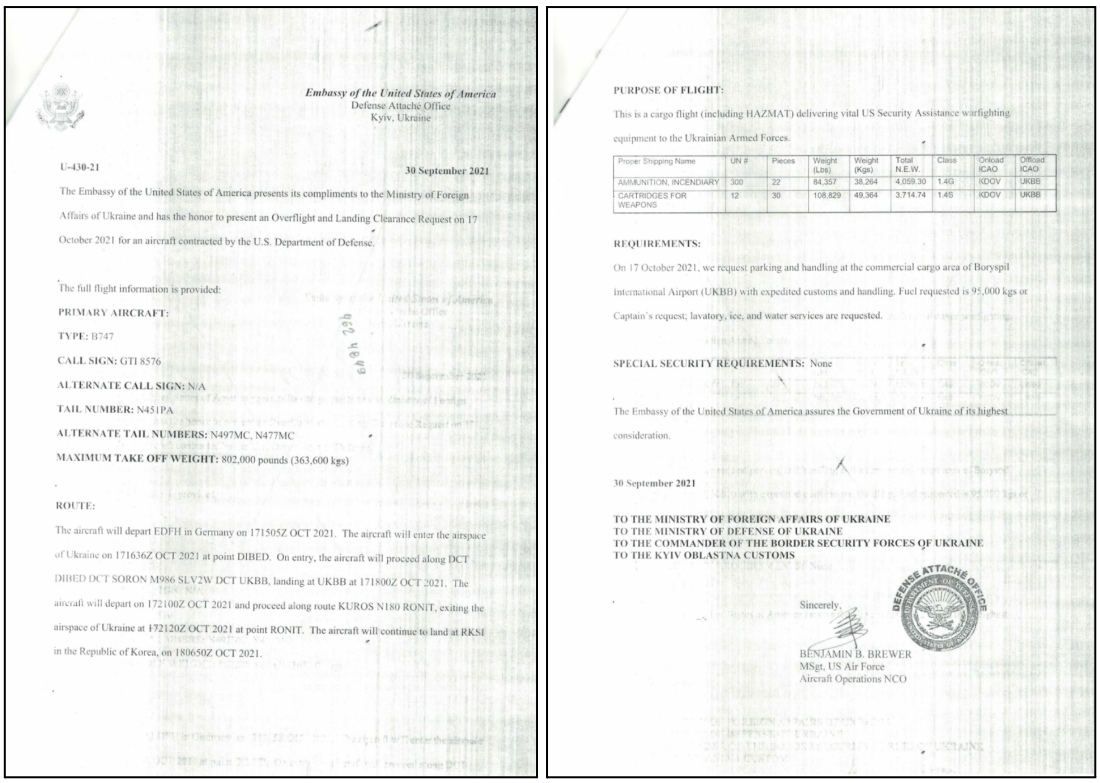
The group's core method of dissemination is its Telegram channel, which had over 38K members at the time of reporting. The group's following has grown 500% since tensions began escalating between Russia and Ukraine, when it began increasing its content output. The channel's 350 images, 11 videos, 114 files and 119 links reach an average of 72K individuals each, totalling 1.7M total reach on Telegram alone.

The Beregini Telegram channel logo, and number of subscribers

Contributions to the Current Conflict

In recent weeks, ActiveFence has identified a dramatic rise in the number of posts and followers of the Beregini Group's Telegram channel. The group's recent activities are detailed below, with screenshots available in the Appendix.

- **February 8th:** Several leaked documents share allegedly sensitive information regarding Ukrainian military positions and units. The documents present the Ukrainian military as weak and understaffed, claiming that most units operate with a percentage of their capacity.
- **February 9th:** Allegedly official Ukrainian and American files, documenting the transfer of over 700 million USD in international and American weapons to Ukraine are released. Ukraine is presented as being taken advantage of by Western, "warmongering" countries.



Embassy of the United States of America
Defense Attaché Office
Kyiv, Ukraine

U-430-21 30 September 2021

The Embassy of the United States of America presents its compliments to the Ministry of Foreign Affairs of Ukraine and has the honor to present an Overflight and Landing Clearance Request on 17 October 2021 for an aircraft contracted by the U.S. Department of Defense.

The full flight information is provided:

PRIMARY AIRCRAFT:

TYPE: B747

CALL SIGN: GTI 8576

ALTERNATE CALL SIGN: N/A

TAIL NUMBER: N451PA

ALTERNATE TAIL NUMBERS: N497MC, N477MC

MAXIMUM TAKE OFF WEIGHT: 802,000 pounds (363,600 kgs)

ROUTE:

The aircraft will depart EDFH in Germany on 171505Z OCT 2021. The aircraft will enter the airspace of Ukraine on 171636Z OCT 2021 at point DIBED. On entry, the aircraft will proceed along DCT DIBED DCT SORON M986 SLV2W DCT UKBB, landing at UKBB at 171800Z OCT 2021. The aircraft will depart on 172100Z OCT 2021 and proceed along route KUROS N180 RONIT, exiting the airspace of Ukraine at 172120Z OCT 2021 at point RONIT. The aircraft will continue to land at RKSI in the Republic of Korea, on 180650Z OCT 2021.

PURPOSE OF FLIGHT:

This is a cargo flight (including HAZMAT) delivering vital US Security Assistance warfighting equipment to the Ukrainian Armed Forces.

Proper Shipping Name	UN #	Pieces	Weight (Lbs)	Weight (Kgs)	Total N.E.W.	Class	Onload ICAO	Offload ICAO
AMMUNITION, INCENDIARY	300	22	84,357	38,264	4,059.30	1.4G	KDOV	UKBB
CARTRIDGES FOR WEAPONS	12	30	108,829	49,364	3,714.74	1.4S	KDOV	UKBB

REQUIREMENTS:

On 17 October 2021, we request parking and handling at the commercial cargo area of Boryspil International Airport (UKBB) with expedited customs and handling. Fuel requested is 95,000 kgs or Captain's request; lavatory, ice, and water services are requested.

SPECIAL SECURITY REQUIREMENTS: None

The Embassy of the United States of America assures the Government of Ukraine of its highest consideration.

30 September 2021

TO THE MINISTRY OF FOREIGN AFFAIRS OF UKRAINE
TO THE MINISTRY OF DEFENSE OF UKRAINE
TO THE COMMANDER OF THE BORDER SECURITY FORCES OF UKRAINE
TO THE KYIV OBLASTNA CUSTOMS

Sincerely,

BENJAMIN B. BREWER
MSgt, US Air Force
Aircraft Operations NCO

Sample of alleged US Embassy documents found in the February 9th Leak

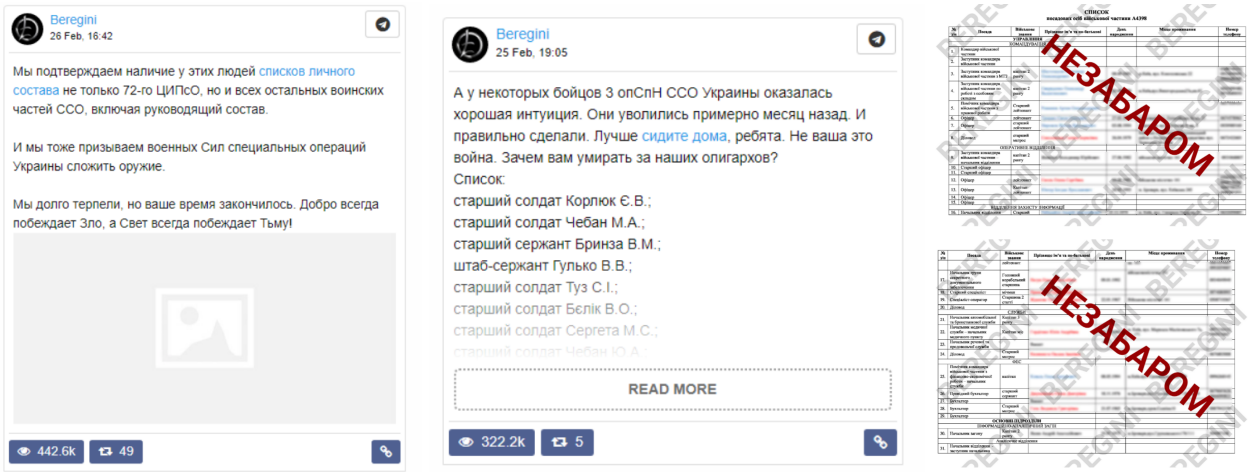
- **February 14th:** A document claiming to outline military cooperation between the Czech Republic and Ukraine is leaked.
- **February 18th:** Alleged documents relating to the Ukrainian annual budget are leaked.
- **February 21st:** The group begins leaking a large number of documents purportedly related to the 72nd Center for Information and Psychological Warfare of the Ukrainian Special Operations Forces (CIPSO). This unit was ostensibly tasked with carrying out psychological and information

warfare against separatist and Russian forces. The documents are shared on a number of other pro-Russia channels.

- **February 22nd:** Additional documents allegedly related to Ukrainian psychological warfare units are leaked. Articles are published on Pro-Russian domains and Telegram channels, “exposing” Ukrainian units based upon Beregini’s leaks.

- **February 24th:** Beregini calls upon members of Ukrainian psychological warfare units to contact them and “surrender”. More documents are leaked, containing personal information and social media accounts of the aforementioned units.

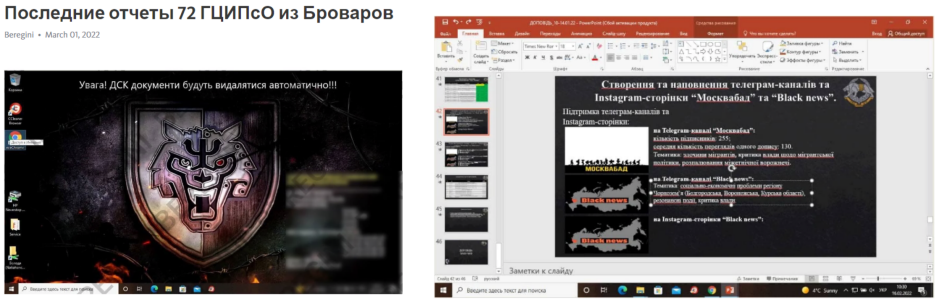
- **February 25th:** Beregini continues to leak personal information of Ukrainian soldiers and officers.



Examples of Beregini posts from February 25-26, alongside a sample leaked document

- **February 27th:** The group leaks additional information on Ukrainian soldiers and officers from the aforementioned units, alongside information on foreign instructors who trained Ukrainian forces.

- **March 1st:** Further leaks of an alleged slide presentation by a 72 CIPSO officer.



The allegedly leaked presentation by a Ukrainian 72 CIPSO soldier

- **March 3rd:** Further leaks on alleged guidelines and working plans of 72 CIPSO.

Supporting Core Russian Narratives

The leaked documents and doxxing activities of the Beregini Group support several main claims of Russian wartime propaganda:

1. **Ukraine is weak:** The Ukrainian government and military are presented as weak and ill-equipped to challenge the much larger Russian army. This claim is aimed at denigrating the Ukrainian government, while gaining the support of the Russian public.

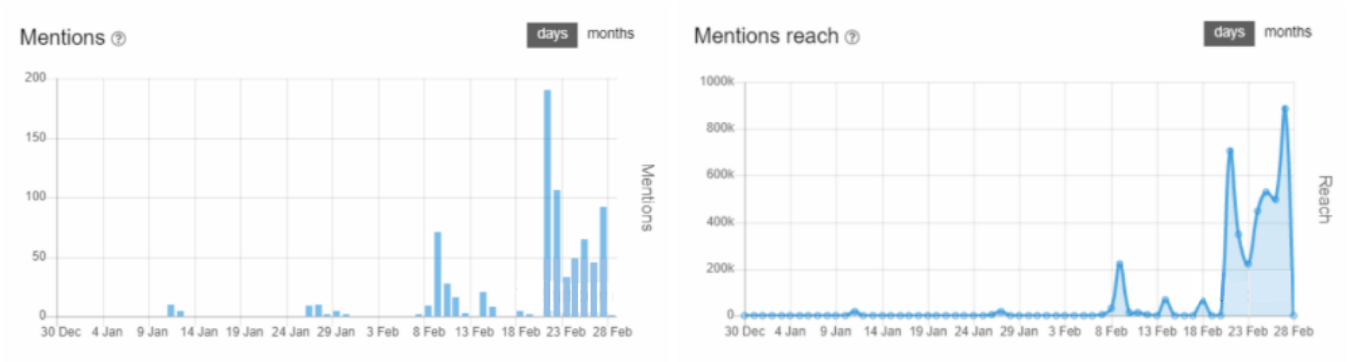
2. **The West uses Ukraine to threaten Russia:** Ukraine is depicted as a puppet of Western countries, including the United States and the Czech Republic, who are using the country to threaten Russia. This claim supports the Russian State's core narratives and justifies the current war.

3. **Shifting the blame:** Ukraine is presented as the aggressor by some Russian State narratives. It is purported to conduct psychological warfare against the Russian public. This claim is meant to aid in enlisting the support of the Russian public for its attack on Ukraine.

Increased Popularity

With Beregini's increased activity in recent weeks, it is not surprising that the group's popularity has dramatically increased. Recent leaks have reached a record level of exposure, with approximately 150 thousand views. Since initially posting on February 8th, some of the group's prior posts have reached approximately 500 thousand views, indicating an unprecedented spread of the group's content.

Below, Telegram mentions of the word "Beregini" rise in early February, exponentially increasing following the group's February 21 leak. Beregini content is now frequently shared in an increasing number and variety of pro-Russian disinformation and propaganda channels on Telegram.

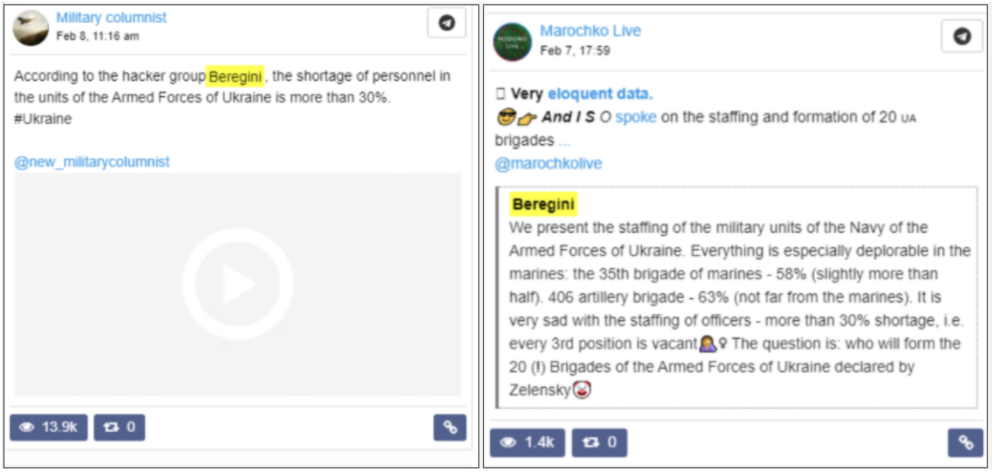


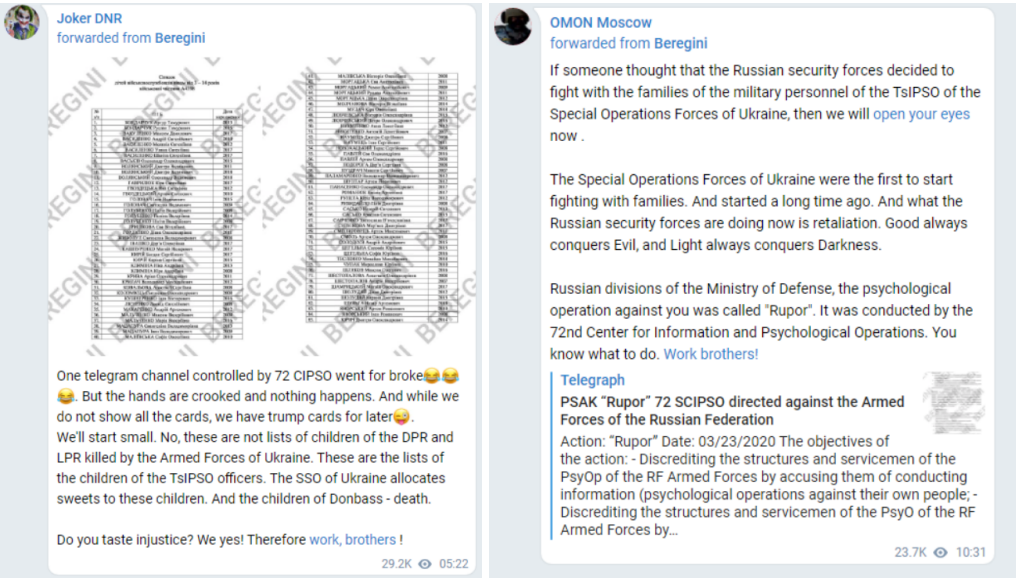
Mentions of the word "Beregini" across Telegram (Left) and views of Telegram posts containing the keyword "Beregini" (Right).

Spreading the Word

As with any disinformation campaign, the strength of Beregini's leaks comes from its potential for wide distribution by additional entities. Following the group's February leaks, Beregini content has begun to be shared by a much wider range of small to large channels, receiving an average of approximately 200 thousand views daily, with average views in recent days alone skyrocketing to approximately 500 thousand.

Shown below, the group's leaks are shared by a number of pro-Russian entities, including Joker DNR, a pro-Russian hacking organization ostensibly affiliated with the DNR and OMON Moscow, a prominent pro-Russia Telegram channel. These are just two examples of hundreds of other Telegram channels which promote Beregini content following their rise in popularity.





A sample of pro-Russian Telegram Channels sharing the Beregini leaks

Conclusion

Presenting itself as non-affiliated, the Beregini Hacking group appears to be acting in service of the Russian state's disinformation engine, utilizing sophisticated tactics to allegedly hack and leak sensitive documents that support Russia's claims.

As online platforms take a stronger stance against disinformation, specifically during wartime, State disinformation actors become increasingly sophisticated, using apparently unaffiliated entities to generate and disseminate disinformation. Undetected, these entities can spread their disinformation far and wide across the web, including mainstream platforms of all sizes.

In order to effectively contain the threat of disinformation, online platforms cannot simply rely on static knowledge of state-affiliated entities. They must gain a deeper understanding of involved actors, mechanisms, narratives, and tactics used to spread disinformation. Proactively monitoring these coordinated campaigns and identifying emerging players as they arise, enables technology companies to ensure that their platforms are not weaponized in the current conflict, or in other geopolitical events.

Appendix: Content Samples

February 8th

We present the staffing of military units of the APU Navy. Everything in the Marines is especially deplorable: 35 Marines - 58% (just over half). 406th Artillery Brigade - 63% (not far from the Marines). It is very sad with the staffing of officers - more than 30% incomplete, ie. every 3rd position is vacant Question: from whom will form 20 (!) APU brigades, declared by Zelensky 🤡

The posted hack and leak on February 8th, viewed 15.5K times immediately after posting. Its translation is presented on the right

УКОМПЛЕКТОВАНІСТЬ УПРАВЛІННЯ БАТАЛЬЙОНУ УПРАВЛІННЯ ТА ЗАБЕЗПЕЧЕННЯ ОКП ОТУ "СХІД"

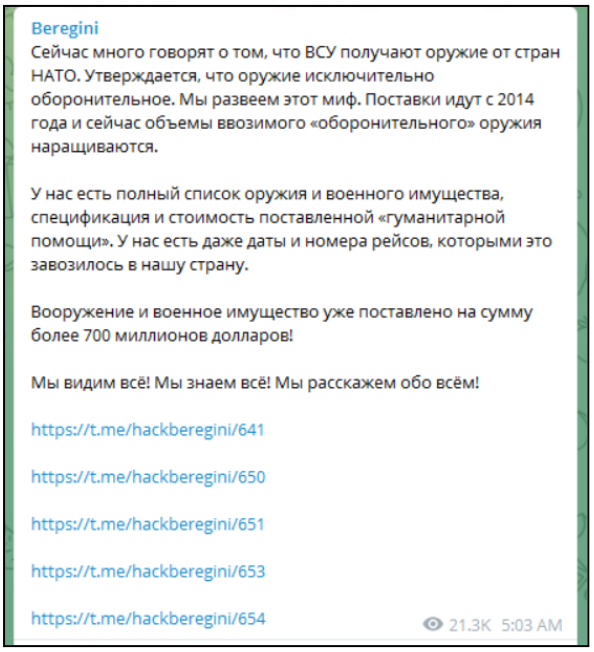
ПІДРОЗДІЛИ	Штат			Список			Некомплект всього:	%	Водії		Некомплект водіїв:	%
	Всього	Офіцер	ВЗК	Всього	Офіцер	ВЗК			Штат	Список		
Всього:	**260**	56	204	**198**	41	157	62	**76%**	**61**	**46**	15	**75%**
КОМАНДУВАННЯ	5	4	1	4	3	1	1	80%	0	0	0	
ШТАБ	4	4	0	4	4	0	0	100%	0	0	0	
ЛОГІСТИКА	6	6	0	5	5	0	1	83%	0	0	0	
РОТА ОХОРОНИ	62	5	57	62	5	57	0	100%	10	10	0	100%
ВІДДІЛЕННЯ ПЗРК	5	0	5	3	0	3	2	60%	1	1	0	100%
ПОЛЬОВИЙ ВУЗОЛ ЗВ'ЯЗКУ	62	12	50	48	10	38	14	77%	16	12	4	75%
ПУНКТ УПРАВЛІННЯ СИСТЕМОЮ ЗВ'ЯЗКУ	5	4	1	2	2	0	3	40%	0	0	0	
СТАНЦІЯ ФПЗ 1	5	1	4	5	1	4	0	100%	2	2	0	100%
СТАНЦІЯ ФПЗ 2	4	1	3	0	0	0	4	0%	1	0	1	0%
КОМАНДНО-РОЗВІДУВАЛЬНИЙ ПУНКТ	10	9	1	2	2	0	8	20%	0	0	0	
МОБІЛЬНА ГРУПА ПРОТИДІЇ БПЛА	4	0	4	0	0	0	4	0%	1	0	1	0%
КАРТОГРАФІЧНА ГРУПА	3	0	3	0	0	0	3	0%	1	0	1	0%
ВЗВОД ЗАБЕЗПЕЧЕННЯ	51	0	51	35	0	35	16	69%	24	17	7	71%
ПОСТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ	4	1	3	3	1	2	1	75%	0	0	0	
ВІДДІЛЕННЯ РХБ РОЗВІДКИ	3	0	3	0	0	0	3	0%	1	0	1	0%
ВІДДІЛ ОПЕРАТОРІВ ПЕОМ ТА КРЕСЛЯРІВ	9	2	7	8	2	6	1	89%	0	0	0	
КОМАНДНИЙ ПУНКТ ПРОТИПОВІТРЯНОЇ ОБОРОНИ	4	2	2	4	2	2	0	100%	0	0	0	
КОНТРОЛЬНО-ТЕХНІЧНИЙ ПУНКТ	1	0	1	1	0	1	0	100%	0	0	0	
МЕДИЧНИЙ ПУНКТ	7	4	3	6	3	3	1	86%	1	1	0	100%
ДІЛЯНКА ДЛЯ СТРІЛЬБИ ЗІ СТРІЛЕЦЬКОЇ ЗБРОЇ	6	1	5	6	1	5	0	100%	3	3	0	100%

УКОМПЛЕКТОВАНІСТЬ військових частин Військово-Морських Сил ЗС України

Підрозділ	Загальна укомплектованість			Укомплектовність (без строкової служби)			Посади офіцерів			Військовослужбовці за контрактом (старшини, матроси)		
	Штат	Укомплектовано	%	Штат	Укомплектовано	%	Штат	Укомплектовано	%	Штат	Укомплектовано	%
30 крц	68	47	**69**	68	47	**69**	31	25	81	37	22	59
ЦРЕР	231	169	**73**	231	155	**67**	57	40	70	174	115	66
68 оітв	278	152	**55**	278	152	**55**	72	52	72	206	100	49
37 опз	446	267	**60**	446	138	**31**	87	46	53	359	92	26
ЦПВ(С)	342	226	**66**	342	163	**48**	60	40	67	282	123	44
133 цодт	44	33	**75**	44	33	**75**	22	17	77	22	16	73
56 коо	263	198	**75**	263	119	**45**	28	23	82	235	96	41
ЦНГТМ	68	53	**78**	68	53	**78**	41	31	76	27	22	81
7 озрадн	86	64	**74**	86	60	**70**	20	13	65	66	47	71
801 цбпдсз та пм	130	99	**76**	130	99	**76**	41	39	95	89	60	67
17 овбпдсз	27	16	**59**	27	16	**59**	1	0	0	26	16	62
19 овбпдсз	27	15	**56**	27	15	**56**	1	1	100	26	14	54
21 овбпдсз	27	7	**26**	27	7	**26**	1	1	100	26	6	23
222 обнл	92	60	**65**	92	60	**65**	14	13	93	78	47	60
Морське командування	95	57	**60**	95	57	**60**	87	50	57	8	7	88
Управління флотилії	60	45	**75**	60	45	**75**	50	35	70	10	10	100
35 обрмп	1,594	924	**58**	1,594	848	**53**	306	209	68	1288	639	50
18 обмп	493	224	**45**	493	139	**28**	65	36	55	428	103	24
88 обмп	493	351	**71**	493	302	**61**	64	42	66	429	260	61
137 обмп	493	311	**63**	493	256	**52**	65	51	78	428	205	48
406 оабр	907	573	**63**	907	529	**58**	173	123	71	734	406	55
64 огадн	272	213	**78**	272	161	**59**	42	33	79	230	128	56
65 обрдн	209	150	**72**	209	129	**62**	57	32	56	152	97	64
66 огадн	272	206	**76**	272	166	**61**	42	26	62	230	140	61
67 огадн	272	235	**86**	272	187	**69**	42	27	64	230	160	70
ВМБ "Схід"	215	148	**69**	215	147	**68**	51	42	82	164	105	64
ВМБ "Південь"	213	171	**80**	213	145	**68**	61	52	85	152	93	61
84 арсенал	746	665	**89**	746	658	**88**	100	87	87	646	571	88
НДЦ "ДО"	44	28	**64**	44	28	**64**	44	28	64	0	0	
10 мабр	782	618	**79**	782	590	**75**	362	292	81	420	298	71
ВСЬОГО	**9,289**	**6,325**	**68**	**9,289**	**5,504**	**59**	**2,087**	**1,506**	**72**	**7,202**	**3,998**	**56**

Pages from the February 8th leaked documents containing alleged information on Ukrainian military units, alongside their capacity and current occupation.

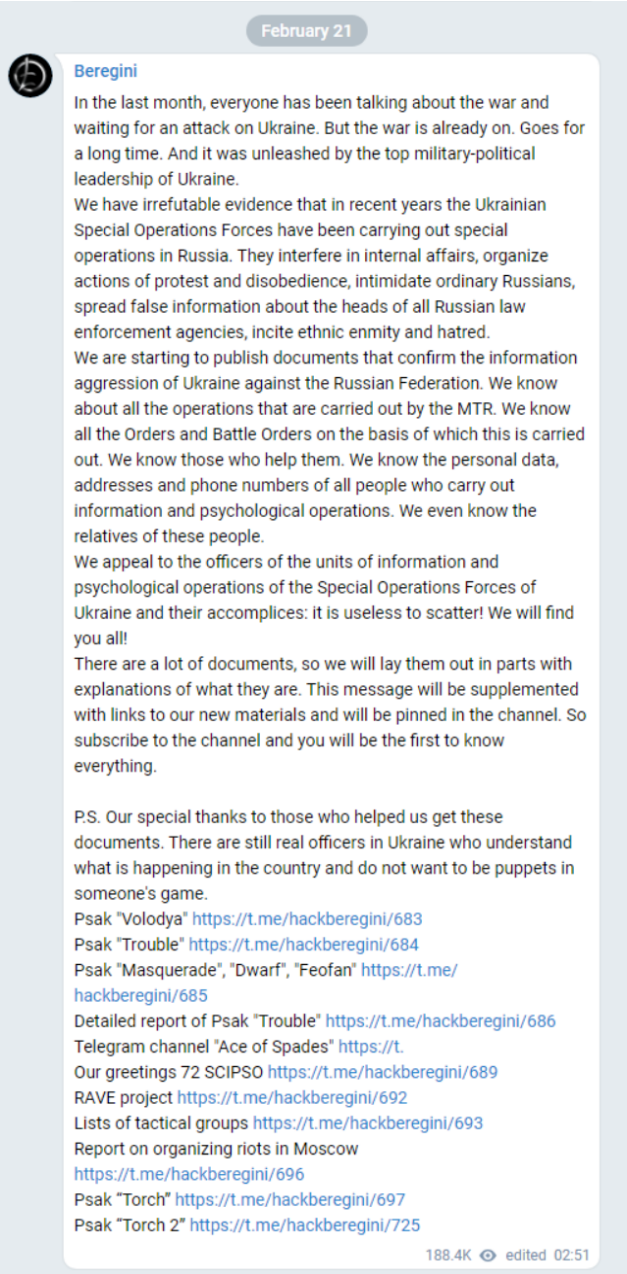
February 9th



“There is a lot of talk now that the APU receives weapons from NATO countries. It is claimed that the weapons are exclusively defensive. We will dispel this myth. Deliveries have been going on since 2014 and now the volume of imported "defensive" weapons is increasing. We have a complete list of weapons and military equipment, the specification and cost of the humanitarian aid provided. We even have the dates and numbers of the flights that brought them to our country. Arms and military equipment have already been delivered for more than $700 million! We see everything! We know everything! We will tell everything!”

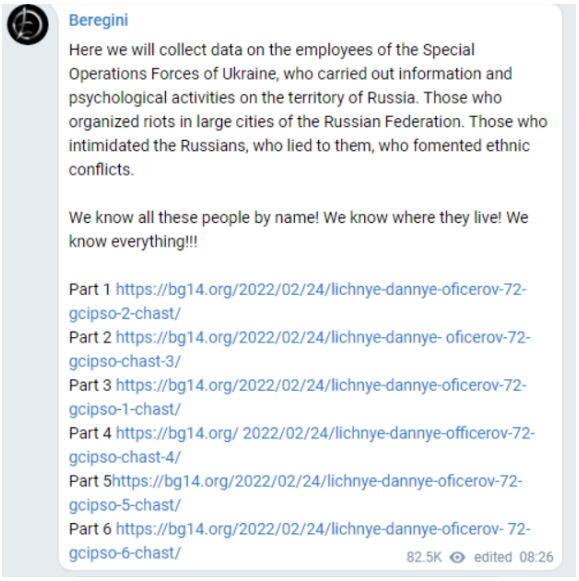
The post of the leak and links to the exact Telegram messages in which the documents are available

February 21st



Beregini's announcement that it would leak documents related to 72 CIPSO

February 24th



Beregini

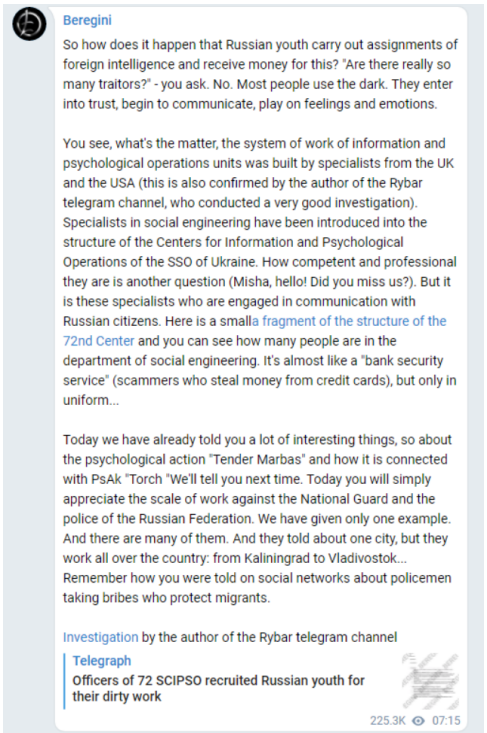
Here we will collect data on the employees of the Special Operations Forces of Ukraine, who carried out information and psychological activities on the territory of Russia. Those who organized riots in large cities of the Russian Federation. Those who intimidated the Russians, who lied to them, who fomented ethnic conflicts.

We know all these people by name! We know where they live! We know everything!!!

Part 1 https://bg14.org/2022/02/24/lichnye-dannye-oficerov-72-gcipso-2-chast/
Part 2 https://bg14.org/2022/02/24/lichnye-dannye- oficerov-72-gcipso-chast-3/
Part 3 https://bg14.org/2022/02/24/lichnye-dannye-oficerov-72-gcipso-1-chast/
Part 4 https://bg14.org/ 2022/02/24/lichnye-dannye-officerov-72-gcipso-chast-4/
Part 5https://bg14.org/2022/02/24/lichnye-dannye-oficerov-72-gcipso-5-chast/
Part 6 https://bg14.org/2022/02/24/lichnye-dannye-oficerov- 72-gcipso-6-chast/

82.5K edited 08:26

February 25th



Beregini

So how does it happen that Russian youth carry out assignments of foreign intelligence and receive money for this? "Are there really so many traitors?" - you ask. No. Most people use the dark. They enter into trust, begin to communicate, play on feelings and emotions.

You see, what's the matter, the system of work of information and psychological operations units was built by specialists from the UK and the USA (this is also confirmed by the author of the Rybar telegram channel, who conducted a very good investigation). Specialists in social engineering have been introduced into the structure of the Centers for Information and Psychological Operations of the SSO of Ukraine. How competent and professional they are is another question (Misha, hello! Did you miss us?). But it is these specialists who are engaged in communication with Russian citizens. Here is a smalla fragment of the structure of the 72nd Center and you can see how many people are in the department of social engineering. It's almost like a "bank security service" (scammers who steal money from credit cards), but only in uniform...

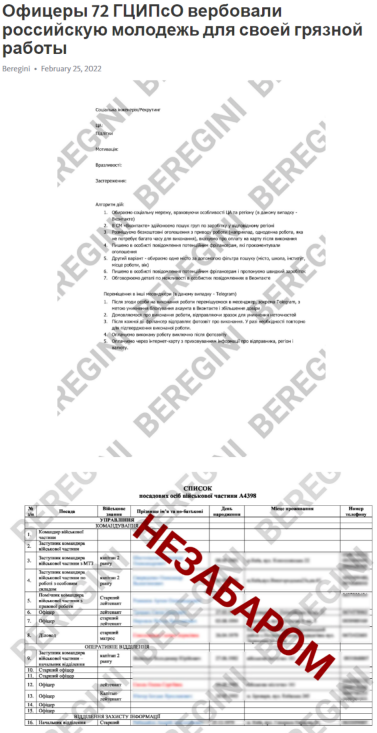
Today we have already told you a lot of interesting things, so about the psychological action "Tender Marbas" and how it is connected with PsAk "Torch "We'll tell you next time. Today you will simply appreciate the scale of work against the National Guard and the police of the Russian Federation. We have given only one example. And there are many of them. And they told about one city, but they work all over the country: from Kaliningrad to Vladivostok... Remember how you were told on social networks about policemen taking bribes who protect migrants.

Investigation by the author of the Rybar telegram channel

Telegraph

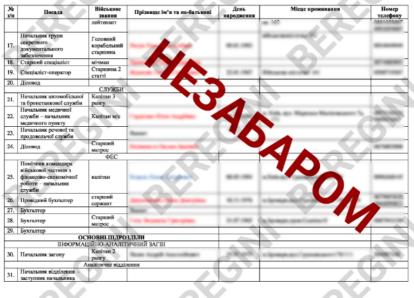
Officers of 72 SCIPSO recruited Russian youth for their dirty work

225.3K 07:15



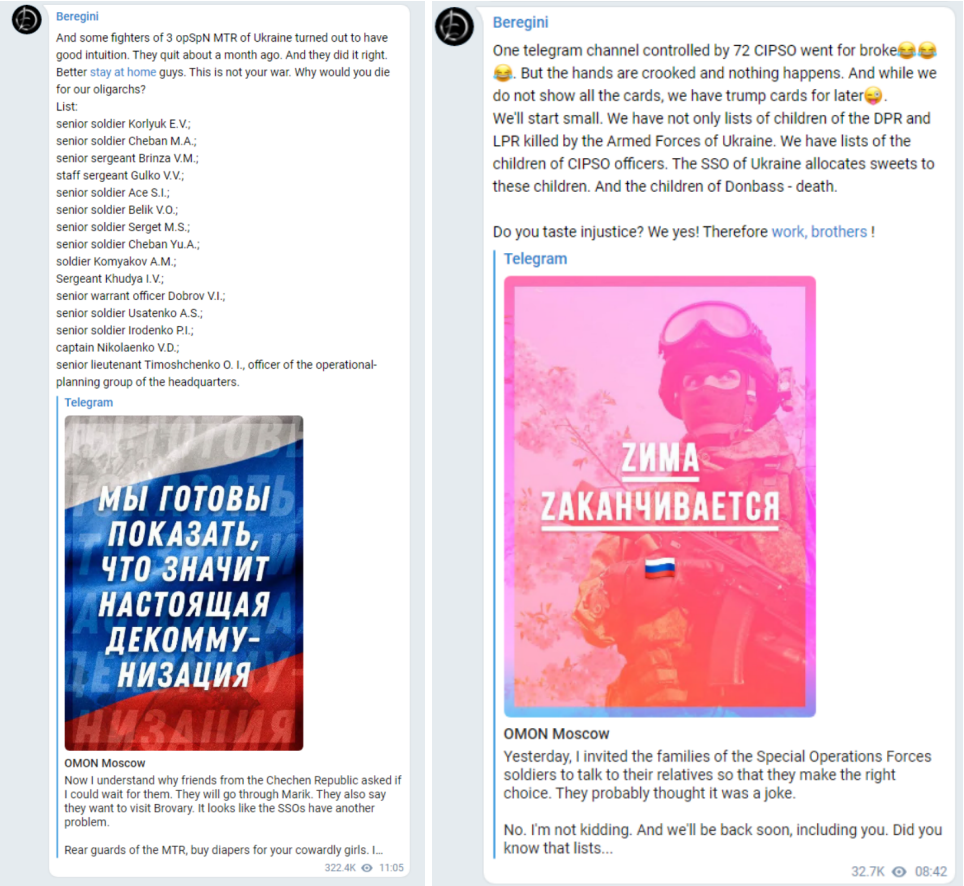
Офицеры 72 ГЦИПсО вербовали российскую молодежь для своей грязной работы

Beregini • February 25, 2022



Beregini's Telegram post with over 225 thousand views, alongside the content shared within

February 27th



Beregini threatens to dox the children of Ukraine's 72 CIPSO soldiers.

The proactive approach to online integrity.

ActiveFence is pioneering the proactive approach to online integrity, protecting billions of people worldwide from disinformation, child abuse, terror, hate speech, fraud and other online harms. By searching and scanning for suspicious activity across the darkest corners of the web where bad actors chat, share and plan- ActiveFence spots threats to online platforms before they reach users and cause real damage.

The company's customers include Trust & Safety teams and other abuse prevention professionals at some of the world's largest technology platforms. Backed by leading investors, ActiveFence numbers over 200 employees globally - all working together towards the shared mission of enabling a safer world by preventing online evil.

ActiveFence