CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

April 6, 2023

Joker DPR and the Information War

Executive Summary

"Joker DPR" is a pro-Russian hacktivist threat group that has risen to prominence during Russia's ongoing invasion of Ukraine. The group is well-known for its historical and current Telegram channels, which it has used to disseminate sensitive information and spread pro-Russian, anti-Ukrainian propaganda. To date, Joker DPR's most significant claim has been an alleged breach of DELTA, a battlefield management system (BMS) that has proven effective for Ukraine's national defense.

Joker DPR's alleged breach was unlikely to have been as wide-reaching as the threat group claimed. Nevertheless, it is part of a growing body of evidence that suggests Joker DPR is deliberately supporting Russia's information war in Ukraine. Based on the alignment of Joker DPR's activities with the goals of Russian influence operations in Ukraine — specifically, undermining support for Ukrainian military and government apparatuses — it is likely that Joker DPR's activities are directed at amplifying Russian information operations in Ukraine, possibly with the coordination of the Russian state.

Key Findings

- Joker DPR has cultivated a sophisticated persona. Although characterized as an individual in its communications, it is likely that Joker DPR is a threat group that relies on a human infrastructure of Ukrainians who sympathize with the Russian cause and like-minded threat actors to gather the sensitive information that it publicizes.
- Joker DPR first appeared on October 21, 2019, with the creation of its first Telegram channel, "Джокер ДНР", which gained over 59,000 subscribers before it was blocked in March 2022.
- Immediately following the forced closure of its first channel, Joker DPR founded a second Telegram channel with the same name. As of this writing, the second "Джокер ДНР" has gained 247,000 subscribers.
- To date, Joker DPR's most significant claim has been an alleged breach of DELTA, a Ukrainian BMS that has proven effective for Ukraine's national defense. However, it is unlikely that this breach was as wide-reaching as Joker DPR claimed.
- It is likely that Joker DPR's information operations and cyber activity are intended to support Russia's information war in Ukraine by eroding public trust in the Armed Forces of Ukraine (AFU) and Ukrainian government, possibly with the coordination or support of the Russian state.

Threat Analysis

"Joker DPR" is a pro-Russian hacktivist group that first appeared on October 21, 2019, and rose to prominence against the backdrop of Ukraine's ongoing war with Russia. The group is well-known for its alleged cyber activities, which have targeted and publicized sensitive information on Ukrainian military and government web resources, and for its social media presence, which it has exploited to disseminate pro-Russian, anti-Ukrainian propaganda.

Despite characterizing itself as "not a person or a group of people … but an idea", Joker DPR's communications often indicate that they were written by a single individual. Regardless of whether one or multiple individuals author Joker DPR's communications, it is likely that Joker DPR is reliant upon a coordinated human infrastructure of Ukrainians who sympathize with Russia and like-minded threat actors to gather the sensitive information that the group publishes. Joker DPR frequently references this network in its communications, boasting that its "spies and hackers" carry out its instructions. On several occasions, Joker DPR has claimed that these agents have provided documentation substantiating allegations of corruption within the Ukrainian government and military, later posted to Joker DPR's communications channels. The documentation appears to be authentic, suggesting that part of Joker DPR's human infrastructure may be embedded within the Ukrainian government or military. Conversely, Joker DPR may simply exaggerate the involvement of Ukrainian actors in its infrastructure as part of a greater attempt to undermine public faith in Ukrainian government and military institutions.

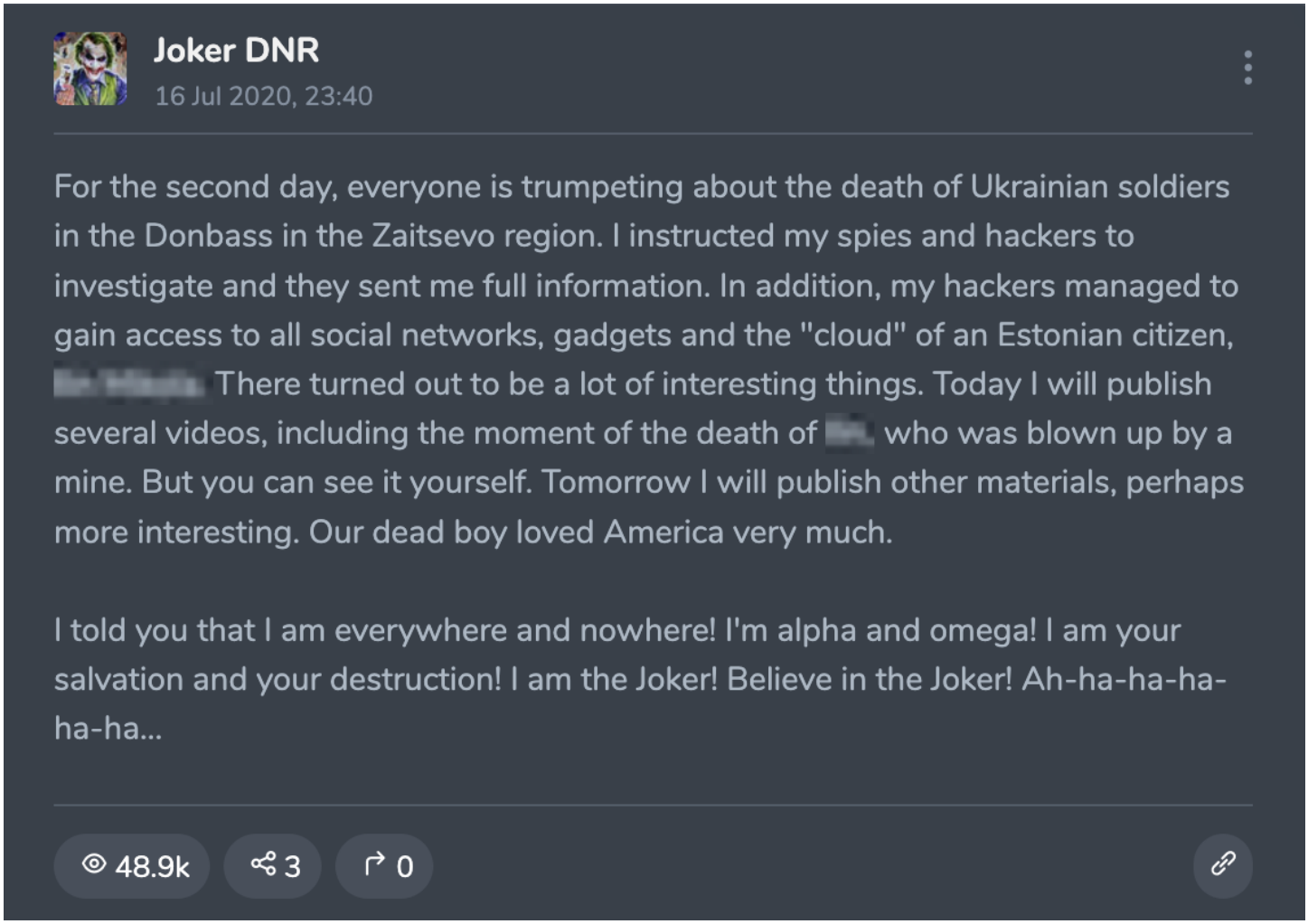

Figure 1: *On its now-defunct Telegram channel, Joker DPR detailed the work of its "spies and hackers". Image text machine-translated from Russian using Google Translate. (Source: TGStat [archive of the blocked Telegram channel Джокер ДНР])*

To a large degree, the mystery of Joker DPR's true identity appears to contribute to its allure: the hacktivist group enjoys great popularity among Russian-language threat actors and has likely garnered support from among Ukrainians with pro-Russian sympathies.

However, not all are content with Joker DPR's current mystique. On November 1, 2022, Vladislav Horohorin, a former cybercriminal with Russian and Ukrainian citizenship, claimed in a post on the Telegram channel "CyberSec's" that Joker DPR was in fact "JokerStash", the former administrator of the defunct dark web carding shop "Joker's Stash".

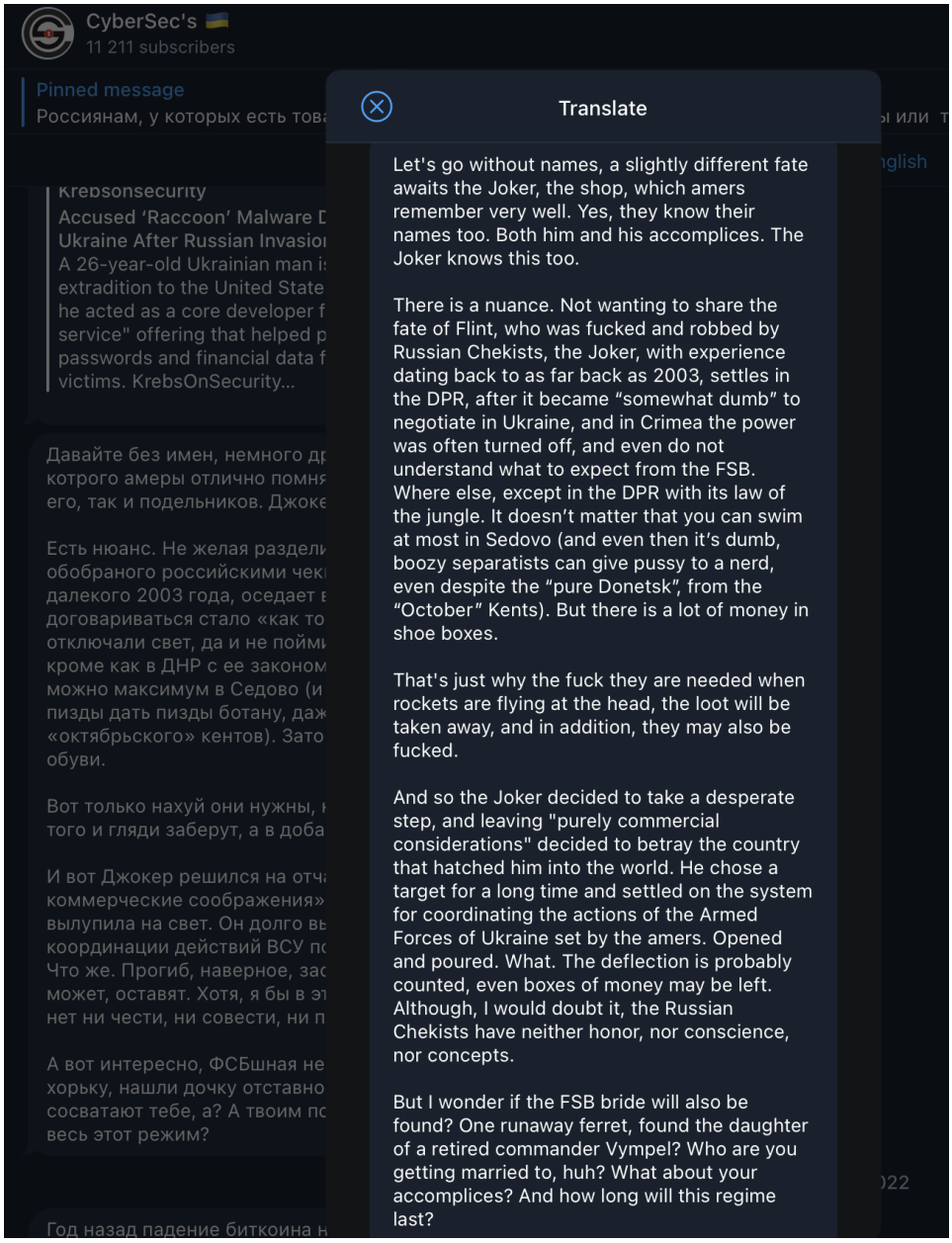

Figure 2: *Vladislav Horohorin laid out his argument for why JokerStash might have taken on the mantle of Joker DPR — image text machine-translated from Russian using Google Translate (Source: Telegram channel CyberSec's)*

Carding shops supply stolen payment card data to criminals seeking to commit payment fraud. Prior to its January 2021 closure, Joker's Stash was the preeminent dark web carding shop: Our data indicates that from April 2017 to January 2021, Joker's Stash earned over $1.1 billion USD in revenue. Similarly, blockchain analysis conducted by a partner institution indicates that from August 2013 to January 2021, Joker's Stash received 284,277 bitcoins (BTC) in over 1.4 million cryptocurrency transactions. While these massive revenues would have offered Joker DPR considerable resources for its activities if it was indeed related to JokerStash, we believe that Horohorin's claim is speculation.

Motivations, Persona, and Name

In its communications, Joker DPR has stated that its mission is to "destroy the clowns" who govern Ukraine and to support the separatist movements in Ukraine's Donbas region. Joker DPR displays a deep distrust for mainstream media and official communications, believing information to be a powerful weapon. The group has described itself as having an obsessive focus on exposing corruption and wrongdoing — particularly within the Ukrainian military. To that end, Joker DPR frequently ridicules Ukrainian leadership, insinuating that the country's resistance against Russian forces would be significantly less successful if not for Western financial, military, and intelligence support.

Since 2019, Joker DPR has carefully cultivated its persona. Its communications style has undergone a metamorphosis, with its early messages focused on personal disparagement and mockery and its most recent messages suggesting a more educated, analytical, and intelligent author or authors. Joker DPR's posts often contain a dark sense of humor and frequent references to violence. This is fitting, as the moniker is a reference to the sociopathic "Joker" character from the "Batman" comics and related franchises, while "DPR" is the English-language abbreviation for the self-proclaimed Donetsk People's Republic, a separatist-controlled region in eastern Ukraine.[1]

Activities

Joker DPR's activities reveal a threat group that has deliberately and enthusiastically supported Russia's information war in Ukraine. Since 2019, Joker DPR has claimed responsibility for various cyber campaigns, including compromises of Ukrainian government and Armed Forces of Ukraine (AFU) web resources. Joker DPR has also released sensitive military information related to the AFU and Ukrainian government through its Telegram channels.

Telegram Channels

Joker DPR first gained notoriety from its original Telegram channel, "Джокер ДНР". There the group published leaks regarding the Ukrainian military from October 2019 to March 2022, when, according to Joker DPR, complaints from Ukrainians forced the channel to close. Before its closure, the original channel accumulated over 59,000 subscribers.

In March 2022, Joker DPR shifted operations to a new Telegram channel bearing the same name. As of this writing, the second Джокер ДНР's following has grown to over 247,000 subscribers. Communications published to the channel have occasionally been referenced by mainstream media outlets.

[1] In Russian-language media, Joker DPR is styled as "Joker DNR". DNR is the Russian-language abbreviation for the Donetsk People's Republic (from Donetskaya Narodnaya Respublika).

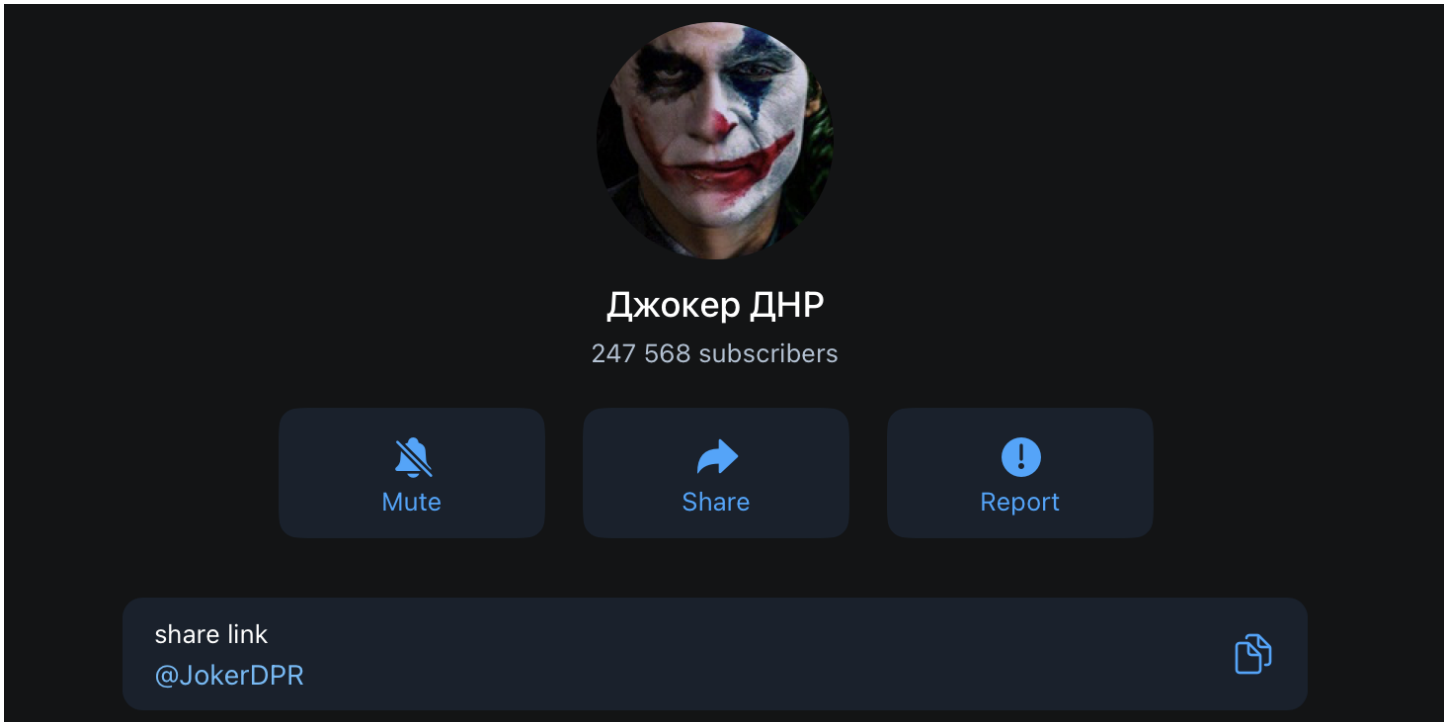

Figure 3: *The second iteration of the Telegram channel "Joker DPR" was created in March 2022 (Source: Telegram channel Джокер ДНР)*

Since 2019, Joker DPR has regularly published threats against the Ukrainian government and military as well as sensitive Ukrainian military information on both of its Telegram channels, including confidential documentation that appears to be authentic, satellite imagery of Ukrainian military bases and materiel caches, and leaks alleging corruption, wrongdoing, or incompetency within the AFU, which are occasionally substantiated with documentation.

To date, Joker DPR's boldest claim has been the alleged compromise of DELTA, a Ukrainian-developed battlefield management system (BMS) that provides military forces with real-time situational awareness regarding both friendly and enemy units.

Alleged Breach of DELTA

On November 1, 2022, Joker DPR claimed that it had successfully penetrated DELTA, asserting that it had gained real-time visibility into the system's use by the AFU. Although the claim was unlikely to be completely true, Russian media quickly picked up the story. The same day, the Ministry of Defense of Ukraine denied that any breach of the DELTA system had occurred, arguing that Joker DPR's claim was part of a psychological operation meant to undermine confidence in DELTA. DELTA is a component in Ukraine's greater network-centric warfare (NCW) doctrine, which places emphasis on rapid, decentralized decision-making.

On November 3, 2022, Joker DPR gained unauthorized access to the Instagram page of General Valeriy Zaluzhny, commander-in-chief of the AFU. The threat group repeated its claim on Zaluzhny's Instagram page.

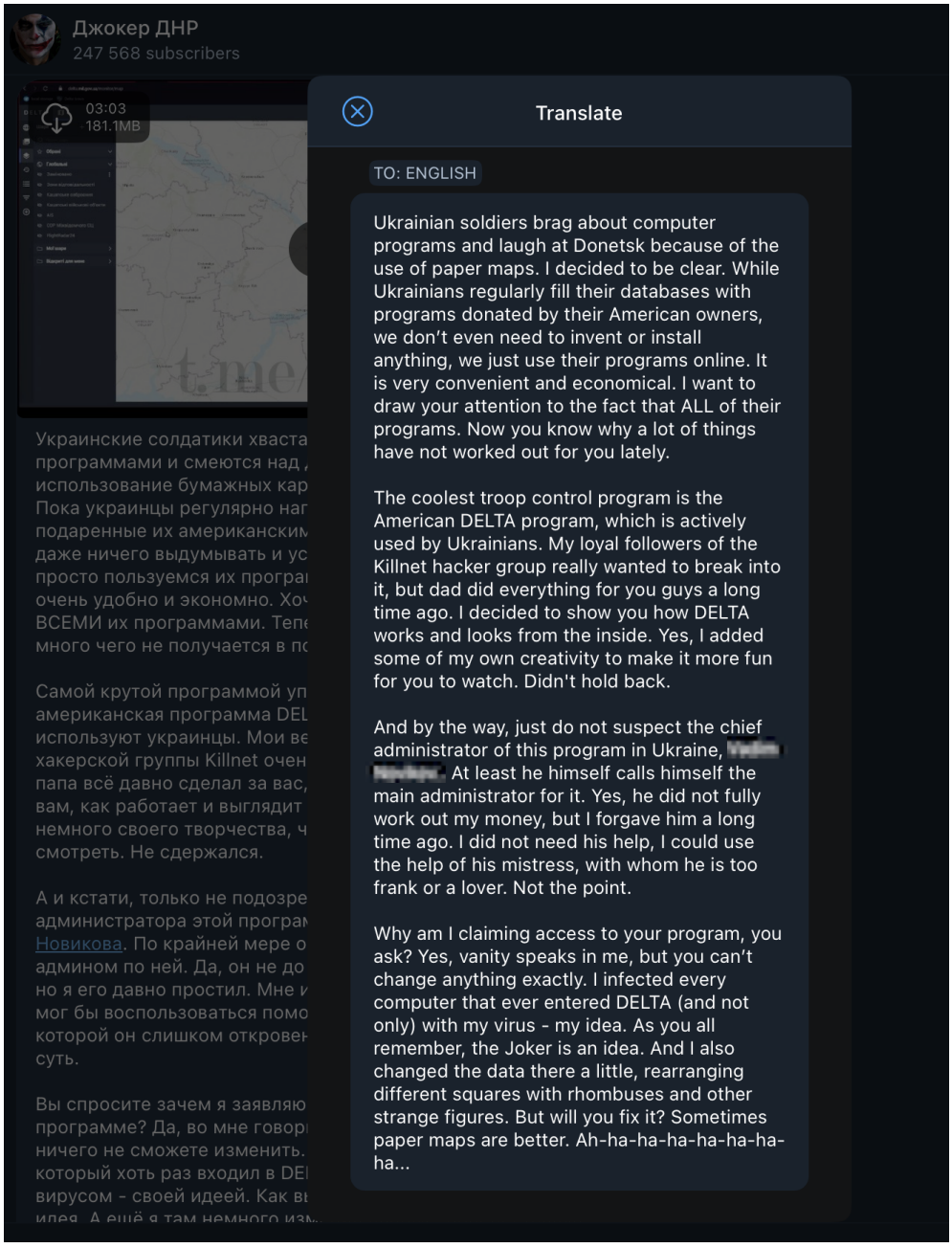

Figure 4: *Joker claimed to have penetrated the Ukrainian-developed BMS DELTA (Source: Telegram channel JokerDPR)*

Although not officially adopted by the AFU until February 4, 2023, DELTA has been in development since 2016 and underwent a significant update just before the onset of the full-scale Russian invasion in February 2022. Ukraine's adoption and execution of NCW was instrumental in repelling early Russian

assaults across key battlegrounds at the start of the invasion; for its part, DELTA played a role in the sinking of the *Moskva*, the flagship of the Russian Black Sea Fleet. Given the role that DELTA continues to play in Ukraine's defense, a wide-reaching compromise of the system would likely have significant implications for the ongoing war in Ukraine and would almost certainly undermine the AFU's ability to conduct coordinated combat operations.

However, Joker DPR's claim of a wide-reaching compromise of DELTA is dubious. By and large, imagery and documents alleged to have been taken from DELTA that were shared in the threat group's Telegram channel were likely accessible from individual user accounts. This suggests that while Joker DPR may have been able to access limited data through insider threats or compromised login credentials, it may not have gained access to the system as a whole.

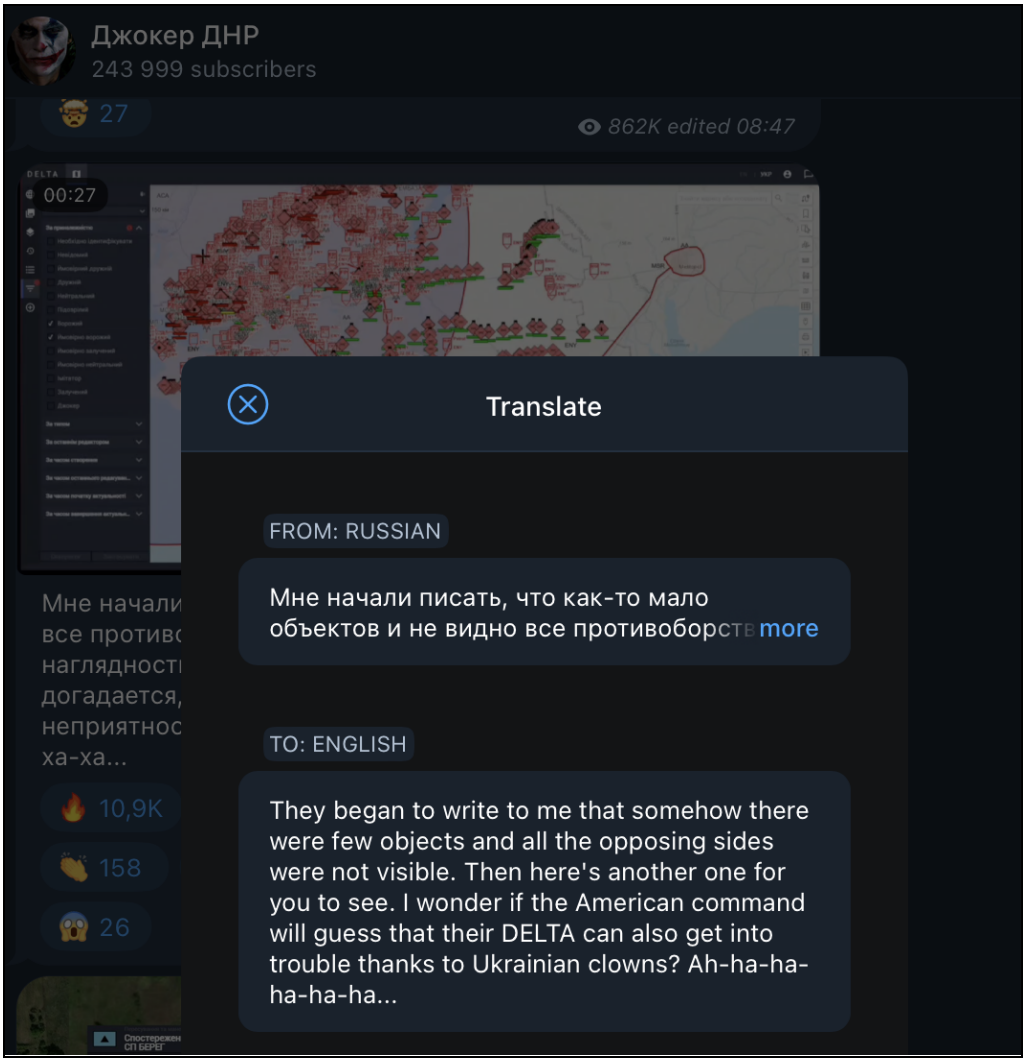

Figure 5: *Joker DPR provided video evidence that it had gained access to DELTA (Source: Telegram channel "JokerDPR")*

Joker DPR's claim is further undermined by the AFU's limited response to the alleged breach. As reported in The Record, cybersecurity is a priority for DELTA developers, who are aware that hostile threat actors routinely target DELTA in recognition of "the danger it poses" to the Russian war effort. Upon learning of Joker DPR's claims, it is likely that the AFU would have conducted a security audit of the BMS. If a serious penetration had been discovered, the AFU likely would have shifted operations to another BMS at its disposal, such as "Kropyva". Moreover, if a serious penetration had occurred, it is unlikely that the AFU would have proceeded with its official adoption of DELTA on February 4, 2023. By the same token, given that Joker DPR has expressed interest in intelligence-sharing with the Russian state, it is unlikely that the threat group would have been so shortsighted as to endanger its access to DELTA with public announcements of the breach.

Lastly, it is unlikely that official Russian media would have embraced Joker DPR's claim so widely if DELTA had actually suffered a serious breach. Russian news media is subject to strict government controls, and deviation from official government directives is not tolerated.[2] If the Russian government had assessed Joker DPR's access to DELTA to be as wide-reaching as it claimed, the media likely would have sought to contain news of the breach in order to provide Russian military and intelligence organs with the opportunity to co-opt and exploit Joker DPR's alleged compromise.

Evidence Suggests Joker DPR Supports Russian Information Operations

It is likely that Joker DPR's activities are directed at supporting and amplifying Russian information operations, possibly in coordination with the Russian state. Such coordination is far from unprecedented, and Joker DPR's actions have demonstrated a deliberate, long-standing alignment with the goals of Russian influence operations in Ukraine.

As discussed in our previous reporting, the threat posed by pro-Russian hacktivists is not in their attacks, but their ability to sow panic and disinformation. Joker DPR's alleged breach of DELTA is only the latest in a long line of communications that have actively supported Russia's information war in Ukraine by undermining trust in Ukrainian military or government institutions. By recirculating the threat group's claim, Russian media — and by extension, the Russian authorities and military — may have intended to erode public trust in an effective Ukrainian asset.

For DELTA, trust is crucial. The system enables rapid battlefield communications, ultimately facilitating quicker decision-making. Creating doubt among Ukrainian commanders to make them hesitant to use or share information to the system would have serious repercussions on the war's outcome.

Russia's possible employment of Joker DPR to further its aims in Ukraine is wholly in line with its current strategic thinking, which observers have dubbed "hybrid warfare" or the "Gerasimov Doctrine". The Gerasimov Doctrine places greater emphasis on cyber and influence operations compared to traditional kinetic operations. In practice, this asymmetrical engagement allows Russia to achieve goals that may have remained unachievable through traditional means.

[2] According to Reporters Without Borders, "almost all independent [Russian] media have been banned, blocked, or declared 'foreign agents'" since Russia's full-scale invasion of Ukraine began.

Quality and Style of Communications

The quality and content published by Joker DPR also indicates that the group's communications may have begun to receive guidance which it previously lacked. Joker DPR's early communications consistently disparage AFU personnel and Ukrainian officials. Their writing style was informal, reliant on colloquialisms, and occasionally marked by spelling or grammatical mistakes. However, Joker DPR's later communications are distinct, polished, and appear to be strategic, with an author who prefers to contextualize and analyze events rather than use them as a springboard for derogatory remarks.

On this basis, it is possible that Joker DPR may have initially begun its activities on its own initiative as an individual, semi-professional, or professional movement. As the channel's influence grew, it is possible that Russian state structures have seen fit to formally or informally develop the threat group — or to increase the resources allocated to the group's activities if the threat group existed as a Russian asset from the start.

Alignment with Other Pro-Russian Hacktivist Threat Groups

Joker DPR's claims of cooperation with other pro-Russian hacktivist threat groups — namely "Beregini", "Sprut", "Limma", and "Killnet" — also suggest that Joker DPR is working alongside the Russian state. Beregini has previously supported Russia's influence operations, and Killnet has expressed its desire to coordinate its operations with the Russian government. Since Russia's full-scale invasion of Ukraine began, Killnet has conducted a series of distributed denial-of-service (DDoS) attacks against government institutions and private businesses located in NATO member states. Similarly, Ukrainian hacktivist Andrey Baranovich has accused Beregini of being directed by Russian special services.

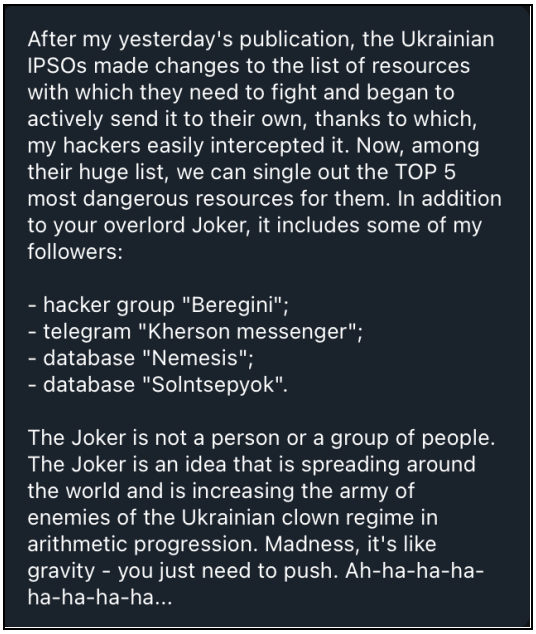

Figure 6: *In a post, Joker DPR listed its "followers", which included Beregini (Source: Telegram channel Джокер ДНР)*

Outlook

Joker DPR will likely continue to engage in information and propaganda operations that undermine trust in the AFU and Ukrainian government, endanger the lives of AFU personnel, and ultimately threaten Ukrainian national security. The potentially far-reaching consequences of Joker DPR's alleged breach of DELTA — specifically, undermining public faith in an asset that has been important to Ukraine's defense — demonstrate that the threat group's activity could affect the outcome of the war in Ukraine.

Joker DPR has built a sizable following on its Telegram channel. As its audience and infrastructure grows, it may gain the increased ability to undermine Ukraine's war effort. Although Ukrainian authorities have not yet targeted Joker DPR, recent events suggest that they will make efforts to identify, arrest, and prosecute members of Joker DPR's network when they have the resources and opportunities to do so, or as the influence and threat level of Joker DPR grows. Although Joker DPR's alleged penetration of DELTA was unlikely to be as wide-reaching as the group claimed, similar activity may lead to the increased international scrutiny of pro-Russian hacktivist threat groups.

Recorded Future®

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture