CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

April 6, 2023

Joker DPRと情報戦争

エグゼクティブサマリー

「Joker DPR」は、ロシアのウクライナ侵攻が続く中で目立つようになった親ロシアのハクティビスト脅威グループです。このグループは、機密情報を広め、親ロシア・反ウクライナのプロパガンダを広めるためにこれまで、そして現在進行形でTelegramチャネルを使用することでよく知られています。今日まで、Joker DPRに関して最も重要な主張は、ウクライナの国防に効果的であることが証明されている戦場管理システム（BMS）であるDELTAの侵害の疑いでした。

Joker DPRの侵害疑惑は、この脅威グループが主張するほど広範囲に及んでいたとは考えにくいものの、Joker DPRがウクライナにおけるロシアの情報戦を意図的に支援していることを示唆する証拠の一部であることは確かです。Joker DPRの活動は、ウクライナにおけるロシアの影響拡大活動の目標（具体的には、ウクライナの軍事組織や政府組織への支援を弱体化すること）と一致していることから、Joker DPRの活動は、おそらくロシア国家の協力を得て、ウクライナにおけるロシアの情報活動を増幅することを目的としているものと思われます。

主な調査結果

- Joker DPRは洗練されたペルソナを培ってきました。その通信においては個人として特徴づけられていますが、ロシアの大義に共感するウクライナ人や志を同じくする脅威アクターによる人的インフラに依存して、機密情報を収集し、公表する脅威グループである可能性があります。
- Joker DPRは、2019年10月21日に最初のTelegramチャンネル「Джокер ДНР」の作成とともに初登場し、2022年3月にブロックされるまでに 59,000人以上の登録者を獲得しました。
- 最初のチャンネルが強制閉鎖された直後、Joker DPRは同じ名前の2番目のTelegramチャンネルを開設しました。この記事の執筆時点で、2番目の「Джокер ДНР」は247,000人のチャンネル登録者を獲得しています。
- 今日まで、Joker DPRの最も重要な主張は、ウクライナの国防に効果的であることが証明されているウクライナのBMSであるDELTAの侵害の疑いでした。ただし、この侵害がJoker DPRの主張ほど広範囲に及んだ可能性は低いです。
- Joker DPRの情報工作やサイバー活動は、ウクライナ軍（AFU）やウクライナ政府に対する国民の信頼を低下させ、ウクライナにおけるロシアの情報戦を支援することを目的としており、おそらくロシア国家の協力や支援を受けているものと思われます。

脅威分析

「Joker DPR」は、2019年10月21日に初めて出現した親ロシア派ハクティビスト集団で、ウクライナとロシアで現在進行中の戦争を背景に有名になりました。同グループは、ウクライナ軍や政府のウェブリソース上の機密情報を狙って公開するサイバー活動や、親ロシア、反ウクライナのプロパガンダを広めるためのソーシャルメディアの悪用でよく知られています。

自らを「個人やグループではなく、概念」であると特徴づけているにもかかわらず、Joker DPRの通信からは、それが1人の個人によって書かれたことがしばしば明らかとなります。Joker DPRの通信を作成するのが一人なのか複数人なのかにかかわらず、Joker DPRは、ロシアに同調するウクライナ人や志を同じくする脅威アクターが連携する人的基盤に基づき、同グループが公表する機密情報を収集していると思われます。Joker DPRは通信の中でこのネットワークに頻繁に言及し、その「スパイとハッカー」が指示を実行していると吹聴しており、何度か、これらのエージェントがウクライナ政府と軍内の汚職の疑いを立証する文書を提供し、後にJoker DPRの通信チャネルに投稿したと主張しました。この文書は本物であるようで、Joker DPRの人的インフラの一部がウクライナ政府または軍に組み込まれている可能性があることを示唆しています。逆に、Joker DPRは、ウクライナ政府と軍事機関に対する国民の信頼を損なうための試みの一環として、インフラへのウクライナ関係者の関与を単に誇張しているだけかもしれません。

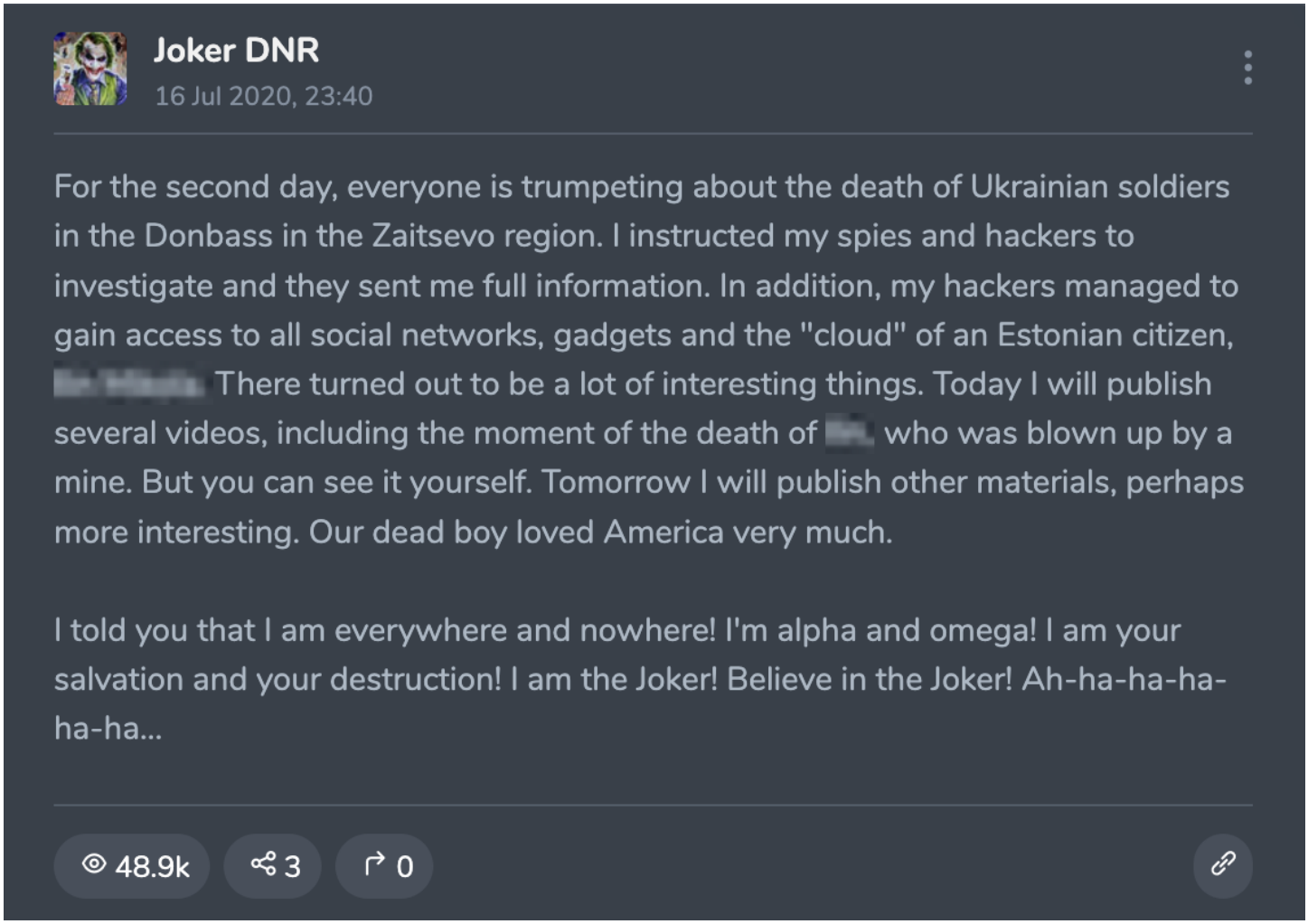

*図**1**: Joker DPRは、現在は機能していないTelegramチャンネルで「スパイとハッカー」の活動を詳説しました。Google翻訳を使ってロシア語から機械翻訳した画像テキスト。(出典: TGStat [ブロックされたTelegramチャンネル Joker DPRのアーカイブ])*

Joker DPRの魅力は、その正体が謎であることも理由のようです。同ハクティビストグループはロシア語話者の脅威アクターの間で人気を博しており、親ロシアの同情を持つウクライナ人の間で支持を集めている可能性があります。

しかし、すべての人が現在のJoker DPRの神秘性に満足しているわけではありません。2022年11月1日、ロシアとウクライナの二重国籍を持つ元サイバー犯罪者のVladislav Horohorinは、Telegramチャンネル「CyberSec's」の投稿で、Joker DPRは実際には、廃止されたダークウェブのカードショップ「Joker's Stash」の元管理者「JokerStash」だと主張しています。

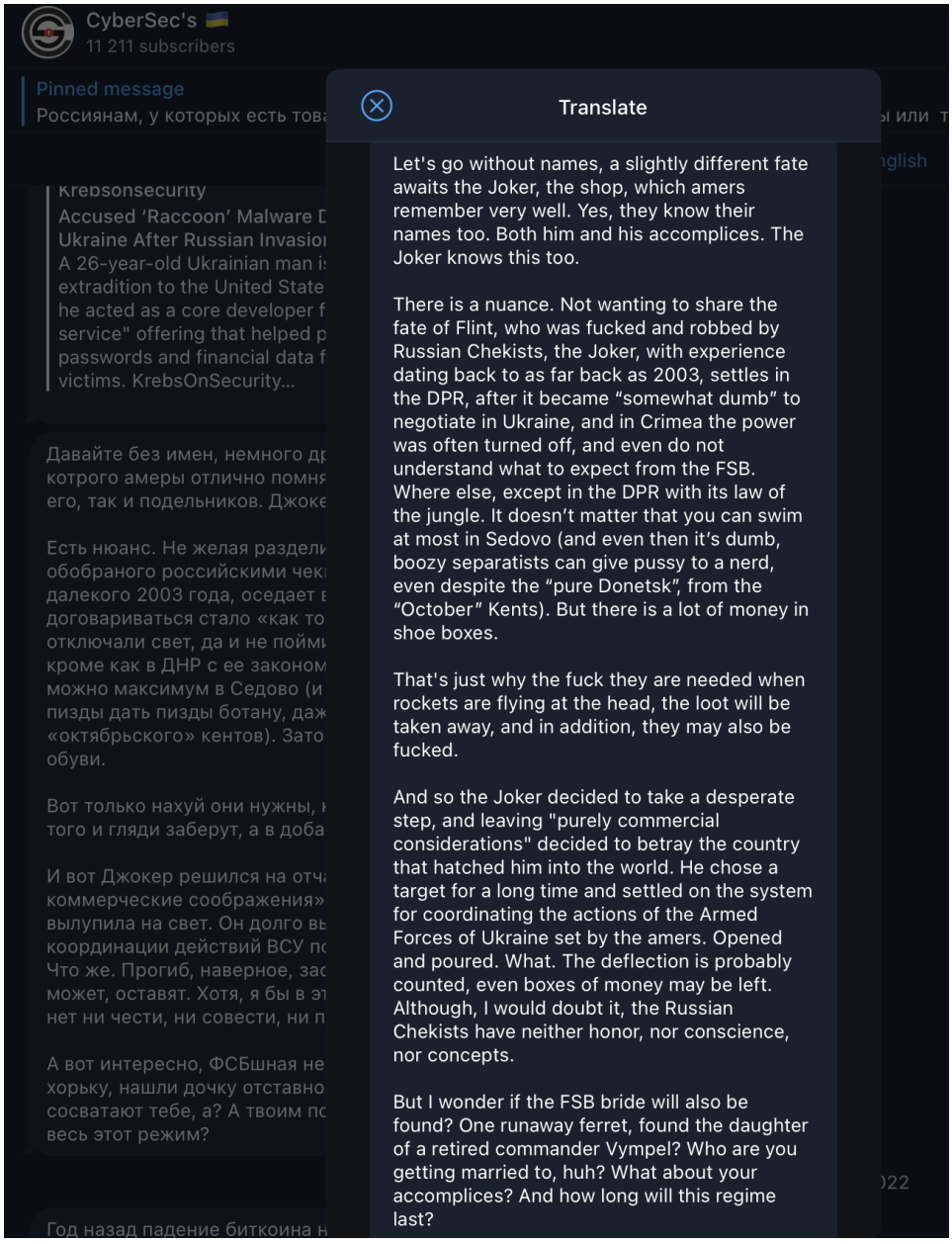

図2：Vladislav Horohorinは、JokerStashがJoker DPRの役割を引き継いだ可能性がある理由を説明しました。Google翻訳を使ってロシア語から機械翻訳した画像テキスト。（出典：TelegramチャンネルCyberSec's）。

カードショップは、盗んだ支払いカードのデータを、支払詐欺を狙う犯罪者に提供します。2021年1月に閉鎖されるまで、Joker's Stashはダークウェブでのカードショップとして傑出していました。当社のデータによると、Joker's Stashは2017年4月から2021年1月までに11億米ドルを超える収益を上げています。同様に、パートナー機関が実施したブロックチェーン分析によると、2013年8月から2021年1月にかけて、Joker's Stashは140万件を超える暗号資産取引で28万4,277ビットコイン（BTC）を受け取ったことが示されています。もし実際にJokerStashが関与しているのであれば、これらの巨額の収益はJoker DPRの活動にかなりのリソースを提供したでしょうが、当社ではHorohorinの主張は憶測であると考えています。

動機、ペルソナ、名前

Joker DPRはその通信の中で、ウクライナを統治する「ピエロを破壊」し、ウクライナのドンバス地域での分離主義運動を支援することが使命であると述べています。Joker DPRは、情報が強力な武器であると信じており、主要メディアや公式のコミュニケーションに対して深い不信感を示しています。同グループは、特にウクライナ軍内の汚職や不正行為を暴露することに執拗な焦点を当てていると自ら説明しており、そのため、頻繁にウクライナ指導部を嘲笑し、西側の財政、軍事、情報機関の支援がなければ、ロシア軍に対する同国の抵抗はこれほど成功しなかっただろうと示唆しています。

2019年以来、Joker DPRはそのペルソナを注意深く育ててきました。そのコミュニケーションスタイルは変貌を遂げており、初期のメッセージでは個人の軽蔑や嘲笑に焦点を当てていながら、最新のメッセージは作者により教養があり、分析的で知的であることを示唆しています。Joker DPRの投稿には、暗いユーモアのセンスが含まれていることが多く、暴力への言及が頻繁です。この名がコミック「バットマン」や関連シリーズに登場する社会病質な「ジョーカー」キャラクターを指し、「DPR」は分離主義者が支配するウクライナ東部の地域の自称ドネツク人民共和国の英語の略称であることからも、このスタンスは適切だと言えます。[1]

活動

Joker DPRの活動からは、ウクライナにおけるロシアの情報戦を意図的かつ熱心に支援してきた脅威グループであることが明らかです。2019年以来、Joker DPRは、ウクライナ政府およびウクライナ軍（AFU）のウェブリソースへの侵害を含む、さまざまなサイバーキャンペーンに対する犯行声明を出しました。また、AFUとウクライナ政府に関連する機密軍事情報をTelegramチャンネルを通じて公開しています。

Telegramチャンネル

Joker DPRは、オリジナルのTelegramチャンネル「Джокер ДНР」で初めて悪名を博しました。そこで同グループは2019年10月から2022年3月までウクライナ軍に関する情報をリークしましたが、Joker DPRでは、ウクライナ人からの苦情によりチャンネルの閉鎖を余儀なくされたとしています。閉鎖されるまで、元のチャンネルの登録者数は59,000人を超えていました。

2022年3月、Joker DPRは同名の新しいTelegramチャネルに運営を移行しました。この記事の執筆時点で、2番目の「Джокер ДНР」のフォロワーは247,000人超に達しています。このチャンネルに公開されたコミュニケーションは、主要メディアに時々参照されることがあります。

[1] ロシア語のメディアでは、Joker DPRは「Joker DNR」と表記されます。DNRは、ドネツク人民共和国（Donetskaya Narodnaya Respublika）のロシア語の略称です。

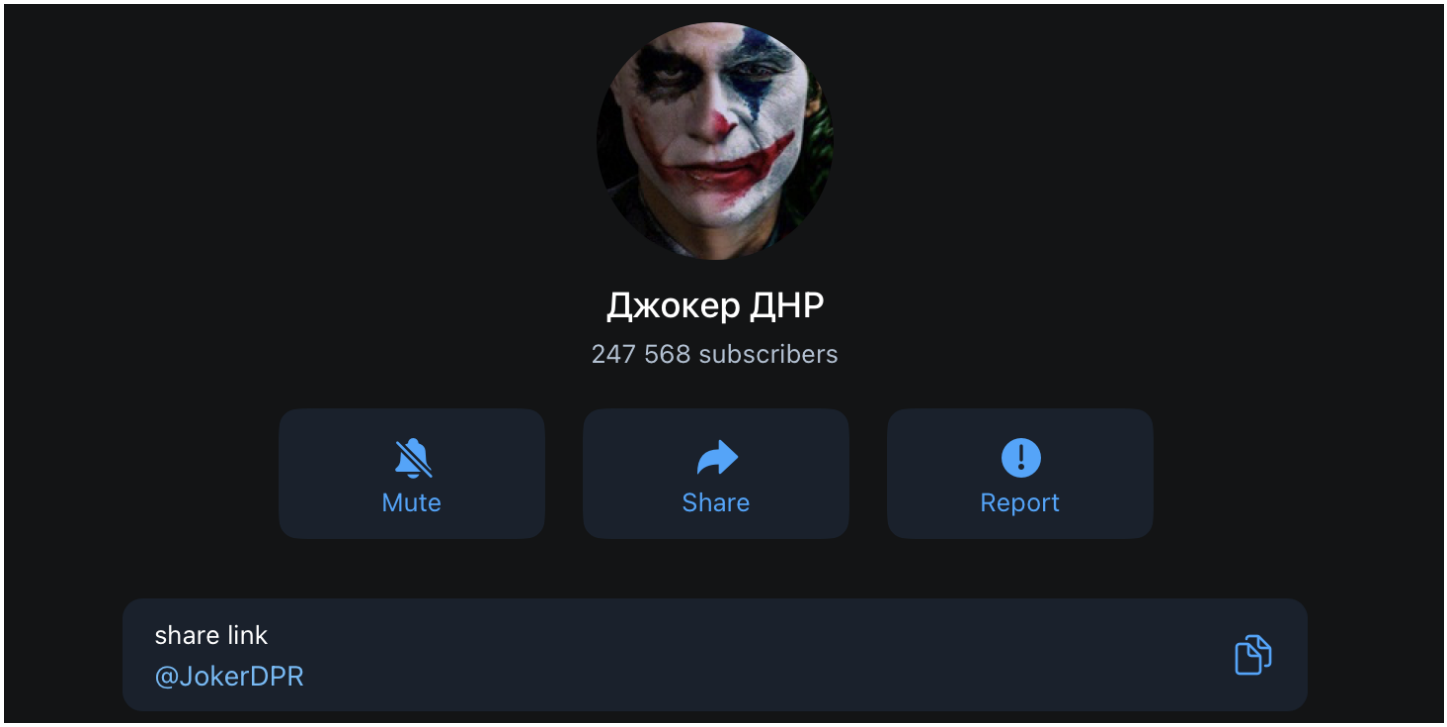

図3：2022年3月にTelegramチャンネル「Joker DPR」の第2弾が誕生しました（出典：Telegramチャンネル Джокер ДНР）

2019年以来、Joker DPRは、ウクライナ政府と軍に対する脅威と、本物と思われる機密文書、ウクライナ軍事基地と物資保管庫の衛星画像、汚職を思わせるリーク情報などのウクライナの機密軍事情報をTelegramチャンネルの両方で定期的に公開してきました。これらはAFU内の汚職、不正行為や無能を主張するもので、文書によって裏付けられることもあります。

これまでのところ、Joker DPRの最も大胆な主張は、DELTA侵害に関するものでした。これは、ウクライナが開発した戦場管理システム（BMS）で、軍隊に味方ユニットと敵ユニットの両方に関するリアルタイムの状況認識を提供します。

DELTA侵害の主張

2022年11月1日、Joker DPRはDELTAへの侵入に成功し、AFUによるシステムの使用状況をリアルタイムで把握できたと主張しました。この主張が完全に真実である可能性は低いものの、ロシアのメディアはすぐにこの話を取り上げました。同日、ウクライナ国防省は、Joker DPRの主張はDELTAへの信頼を損なうことを意図した心理作戦の一部であると主張し、DELTAシステムへの違反が起こったことを否定しました。DELTAは、迅速かつ分散化された意思決定に重点を置く、ウクライナの広範なネットワーク中心戦争（NCW）ドクトリンの構成要素です。

2022年11月3日、Joker DPRはAFUの最高司令官Valeriy Zaluzhny将軍のInstagramページへの不正アクセスを取得し、同氏のInstagramページで自身の主張を繰り返しました。

*図**4**：Jokerはウクライナの開発したBMS DELTAへの侵入を主張しました（出典：Telegramチャンネル JokerDPR）*

AFUによる正式採用は2023年2月4日となりますが、DELTAは2016年から開発されており、2022年2月にロシアの侵攻が本格的に始まる直前に大幅な更新が行われました。ウクライナのNCWの採用と実行は、侵略開始時に主要な戦場を横断する初期のロシアの攻撃を撃退するのに役立ちました。また、DELTAはロシアの黒海艦隊の旗艦であるMoskvaの*沈没*にも寄与しました。DELTAがウクライナの防衛において引き続き果たしている役割を考えると、広範囲にわたるシステムの侵害は、ウクライナで進行中の戦争に重大な影響を与える可能性が高く、調整された戦闘作戦を実施するAFUの能力を損なうことはほぼ確実です。

ただ、広範囲にわたるDELTAの侵害に関するJoker DPRの主張は疑わしいと考えられます。脅威グループのTelegramチャネルで共有されたDELTAから取得されたとされる画像や文書は、一般に、個々のユーザーアカウントからアクセスが可能と考えられ、これは、Joker DPRが内部者脅威や侵害されたログイン資格情報によって一部のデータにアクセスできた可能性を示唆し、一方でシステム全体にアクセスできなかった可能性があることを示しています。

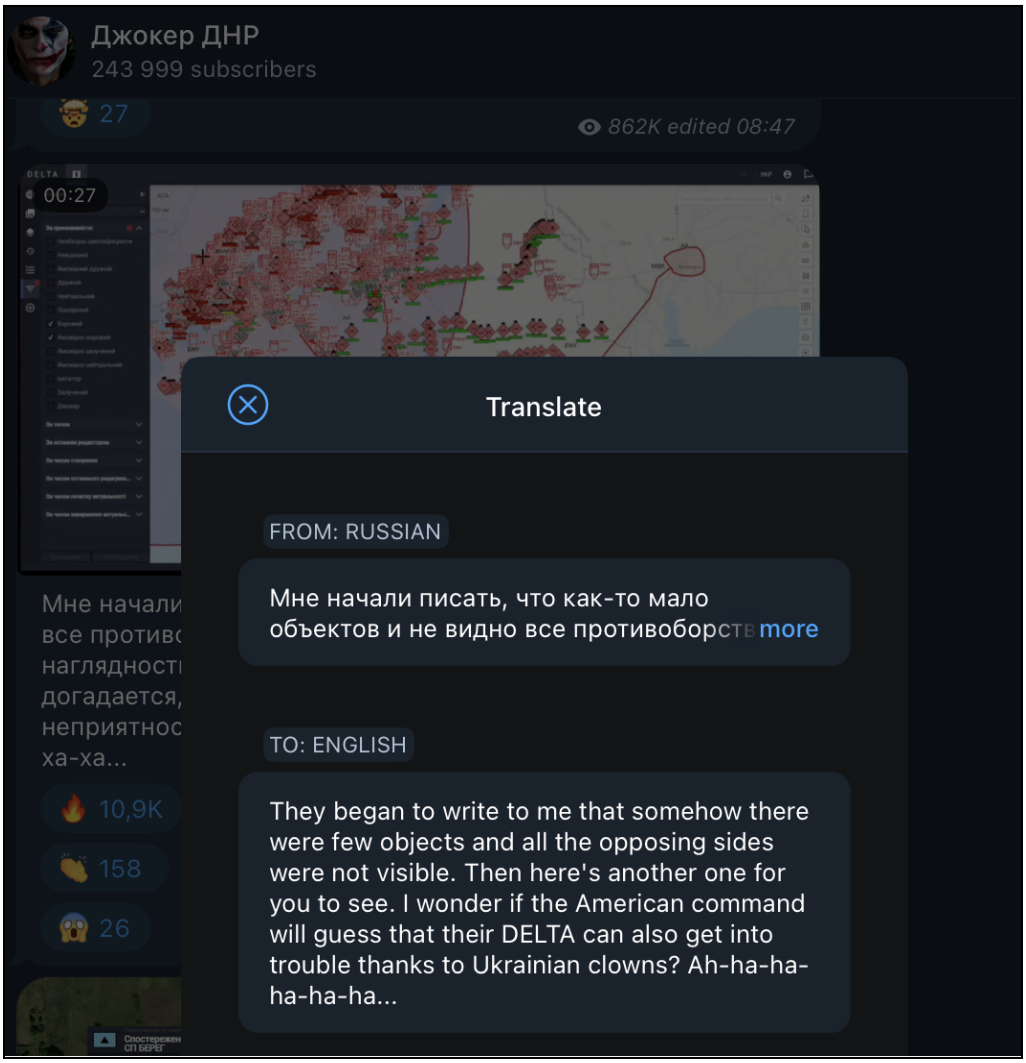

*図**5**: Joker DPRはDELTAにアクセスしたことを示す証拠映像を提供しました（出典：Telegramチャンネル「JokerDPR」）*

Joker DPRの主張の信頼性は、侵害の申し立てにAFUの対応が限定的なことでさらに損なわれています。The Recordで報告されているように、サイバーセキュリティはDELTA開発者にとって優先事項であり、敵対的な脅威アクターが対ロシアの戦術に「もたらす危険」から、DELTAを日常的に標的にしていることを認識しています。Joker DPRの主張を知ったAFUは、BMSのセキュリティ監査を実施した可能性があります。深刻な侵入が発見された場合、AFUは「Kropyva」などの利用可能な別のBMSに運用をシフトした可能性があります。また、深刻な侵入が発生していたとしたら、AFUが2023年2月4日にDELTAの正式採用を進めた可能性は低いでしょう。同様に、Joker DPRがロ

シア国家との情報共有に関心を示していることを考えると、同グループが侵害を公に発表してDELTAへのアクセスを危険にさらすほど近視眼的であった可能性は低いと考えられます。

最後に、もしDELTAが実際に重大な侵害を受けていたとすれば、ロシアの公式メディアがJoker DPRの主張をここまで広く取り上げた可能性は低いです。ロシアのニュースメディアは厳格な政府管理下にあり、政府の公式指令からの逸脱は容認されません。[2]もし、ロシア政府がJoker DPRのDELTAへのアクセスがその主張ほど広範囲であると評価していたら、メディアは、ロシアの軍と諜報機関にJoker DPRの侵害の疑いを取り入れて悪用する機会を提供するために、違反のニュースを封じ込めようとした可能性が高いでしょう。

Joker DPRがロシアの情報作戦を支援していることを示唆する証拠

Joker DPRの活動は、おそらくロシア国家と連携して、ロシアの情報活動を支援し、増幅させることを目的としていると思われます。このような連携には前例が多数あり、Joker DPRの行為は、ウクライナにおけるロシアの影響力拡大活動の目標と意図的かつ長期的に連携していることを示すものです。

以前のレポートで説明したように、親ロシアのハクティビストのもたらす脅威は、その攻撃ではなく、パニックと偽情報を撒き散らす能力にあります。Joker DPRのDELTA侵害の疑いは、ウクライナの軍隊や政府機関への信頼を損なうことでウクライナでのロシアの情報戦争を積極的に支援してきた一連のストーリーのごく一部に過ぎません。脅威グループの主張を再流布することにより、ロシアのメディア、ひいてはロシア当局と軍が、ウクライナの有効な資産に対する国民の信頼を損なうことを狙っていた可能性があります。

DELTAにとって信頼は非常に重要です。このシステムは戦場での迅速なコミュニケーションを可能にし、最終的にはより迅速な意思決定を促進します。ウクライナの司令官の間に疑惑を引き起こし、システムへの情報の使用や共有をためらわせれば、戦争の結果に重大な影響を与えるでしょう。

ロシアがウクライナでの目的推進のためにJoker DPRを利用する可能性は、関係者が「ハイブリッド戦争」または「ゲラシモフ・ドクトリン」と呼んでいる現在の戦略的思考と完全に一致しています。ゲラシモフ・ドクトリンとは、従来の物理的作戦と比較して、サイバー作戦や影響力拡大作戦に重点を置いたものです。実際に、こうした作戦の採用により、ロシアは従来の手段では達成できなかった可能性のある目標を達成することができます。

コミュニケーションの質とスタイル

Joker DPRによって公開された品質とコンテンツからは、グループのコミュニケーションに以前はなかったガイダンスが反映され始めた可能性があることも示しています。Joker DPRの初期の発信は一貫してAFU職員とウクライナ当局者を軽蔑するもので、文体はくだけたもので、口語表現が多く、スペルや文法の間違いが時折見られました。しかし、Joker DPRのその後の発信は独特かつ洗練されており、軽蔑的な発言の舞台としてプラットフォームを使用するのではなく、事象を文脈化して分析することを好む傾向にあり、戦略的であるように見えます。

このことから、Joker DPRは当初、個人、セミプロ、プロによる動きとして、自らの意思で活動を開始した可能性があるものと思われます。このチャンネルの影響力が高まるにつれ、ロシアの国家機構が同脅威グループを公式・非公

[2]Reporters Without Bordersによると、ロシアのウクライナ全面侵攻が始まって以来、「ほとんどすべての独立した[ロシアの]メディアは禁止、ブロック、または『外国のエージェント』と宣言されています」。

式に発展させる、あるいは同グループが最初からロシアの影響下にあった場合、グループの活動に割り当てられるリソースを増やすことが適切だと考えた可能性があります。

他の親ロシア派ハクティビスト脅威グループとの連携

Joker DPRが他の親ロシアのハクティビスト脅威グループである「Beregini」、「Spru」、「Limma」、「Killnet」と協力しているという主張も、Joker DPRのロシア国家との協力を示唆しています。Bereginiは以前、ロシアの影響力拡大作戦を支援しており、Killnetはロシア政府との作戦調整の意向を表明しています。ロシアのウクライナ侵攻が本格的に始まって以来、KillnetはNATO加盟国の政府機関や民間企業に対して一連の分散型サービス拒否（DDoS）攻撃を行ってきました。同様に、ウクライナのハクティビストAndrey Baranovichは、Bereginiがロシアの特殊サービスから指示を受けていると非難しています。

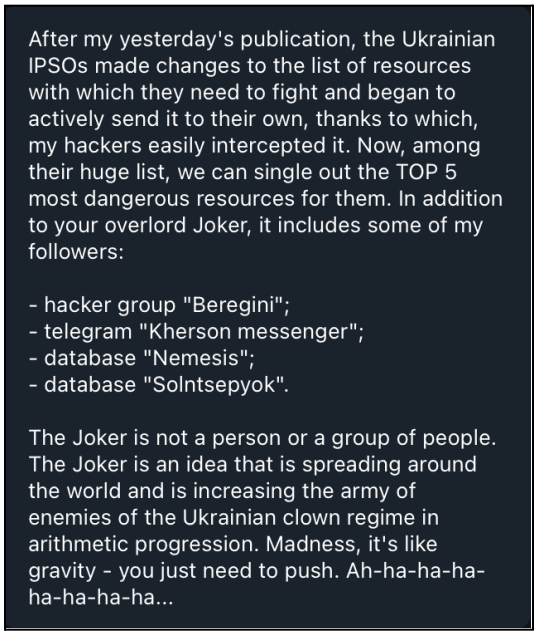

*図**6**: Joker DPRは投稿の中でBereginiを含む「フォロワー」をリストアップしています（出典：Telegramチャンネル Джокер ДНР）*

今後の展望

Joker DPRは今後も、AFUとウクライナ政府への信頼を損ない、AFU職員の命を危険にさらし、最終的にはウクライナの国家安全保障を脅かす情報・宣伝活動に従事し続ける可能性が高いと考えられます。Joker DPRのDELTA侵害の主張が潜在的に及ぼす影響の大きさ、具体的には、ウクライナの防衛にとって重要な資産に対する国民の信頼の失墜は、この脅威グループの活動がウクライナでの戦争の結果に影響を与える可能性があることを示しています。

Joker DPRはTelegramチャンネルでかなりのフォロワーを獲得しており、視聴者とインフラが増えるにつれて、ウクライナの戦争への取り組みを弱体化させる能力が高まる可能性があります。ウクライナ当局はまだJokerDPRを標的にしていませんが、最近の事象から、リソースと機会があれば、またはJoker DPRの影響力と脅威のレベルが高まれば、Joker DPRのネットワークのメンバーの特定、逮捕、起訴に動くことが示唆されています。Joker DPRが主張するDELTAへの侵害は、同グループの主張ほど広範囲に及ぶ可能性は低いですが、同様の活動により、親ロシアのハクティビスト脅威グループに対する国際的な監視が強化される可能性があります。

*Insikt Group®*について

Insikt GroupはRecorded Futureの脅威調査部門です。政府、法執行機関、軍、情報機関での豊富な経験を持つアナリストとセキュリティ研究者が在籍しています。その使命は、幅広いサイバー脅威と地政学的脅威についてのインテリジェンスをもたらして、お客様のリスクを軽減し、具体的な成果を上げ、ビジネスの中断を防ぐことです。国家支援型の脅威グループ、ダークネットや犯罪者が集まるアンダーグラウンドで金銭を目的として活動する脅威アクター、新しいマルウェアと攻撃者のインフラストラクチャ、戦略地政学、影響工作などについて調査しています。

*Recorded Future®*について

Recorded Futureは、世界最大規模のインテリジェンス企業です。Recorded Futureのクラウドベースインテリジェンスプラットフォームは、攻撃者、インフラストラクチャ、標的を包括的にカバーしています。Recorded Futureは、継続的かつ広範な自動でのデータ収集と分析を人による分析を組み合わせることで、広大なデジタル空間をリアルタイムで可視化し、お客様が事前対策により攻撃を阻止して、自社に関わる人々、システム、インフラストラクチャの安全を守れるよう支援します。ボストンに本社を置き、世界中にオフィスおよび従業員を擁するRecorded Futureは、60か国以上、 1,500を超える企業や政府機関と連携しています。

詳しくはrecordedfuture.comを参照するか、Twitterで@RecordedFutureでフォローしてください。