

# GRU: Rise of the (Telegram) MinIOs

Cyber Espionage (CE)

Critical Infrastructure (CI)

Fusion (FS)

Hacktivism (HK)

Strategic (ST)

August 3, 2022 03:51:55 PM, 22-00017174, Version: 1

## Executive Summary

- Mandiant is tracking multiple self-proclaimed hacktivist groups working in support of Russian interests. These groups primarily have conducted distributed denial-of-service (DDoS) attacks and leaked stolen data from victim organizations. Although some of these actors are almost certainly operating independently of the Russian state, we have identified multiple so-called hacktivist groups whose moderators we suspect are either a front for or operating in coordination with the Russian state.
- We assess with moderate confidence that moderators of the purported hacktivist Telegram channels XakNet Team, Infocentr, and CyberArmyofRussia\_Reborn are coordinating their operations with Russian Main Intelligence Directorate (GRU)-sponsored cyber threat actors. Our assessment is based in part on the deployment of GRU-sponsored APT28 tools on the networks of Ukrainian victims whose data was subsequently leaked on Telegram within 24 hours of wiping activity by APT28, as well as other indicators of inauthentic activity by the moderators and similarities to previous GRU information operations.
- The war in Ukraine has also presented novel opportunities to understand the totality, coordination, and effectiveness of Russian cyber programs, including the use of social media platforms by threat actors. Additionally, platforms such as Telegram were being used pre-invasion to influence perception of the impending Russian military movements and have been employed heavily by both Ukraine and Russia to influence both international and domestic audiences.

## Threat Detail

Mandiant is tracking multiple groups claiming to be hacktivists that have targeted Ukraine since the start of the Russian invasion in early 2022. In particular, Mandiant has focused on analyzing a set of self-proclaimed hacktivist groups: XakNet Team, Infocentr, and CyberArmyofRussia\_Reborn. Through our analysis, Mandiant has identified new evidence connecting the moderators of these groups to the Russian state, including timeline analysis of intrusions and leaks from Ukrainian organizations. Mandiant has also [identified limited](#) links between XakNet Team and the pro-Russia so-called "hacktivist" group KillNet, and we assess with moderate confidence that XakNet and KillNet have directly coordinated some of their activity. However, we note that the two appear to conduct aligned but separate missions, based on the observed activity claimed by each of the "hacktivist" groups. While we continue to separately investigate KillNet, this report's scope is limited to the three groups we have currently identified as linked to the GRU.

## Suspected False Hactivist Fronts Leaked Data Likely Stolen From APT28 Wiper Victims

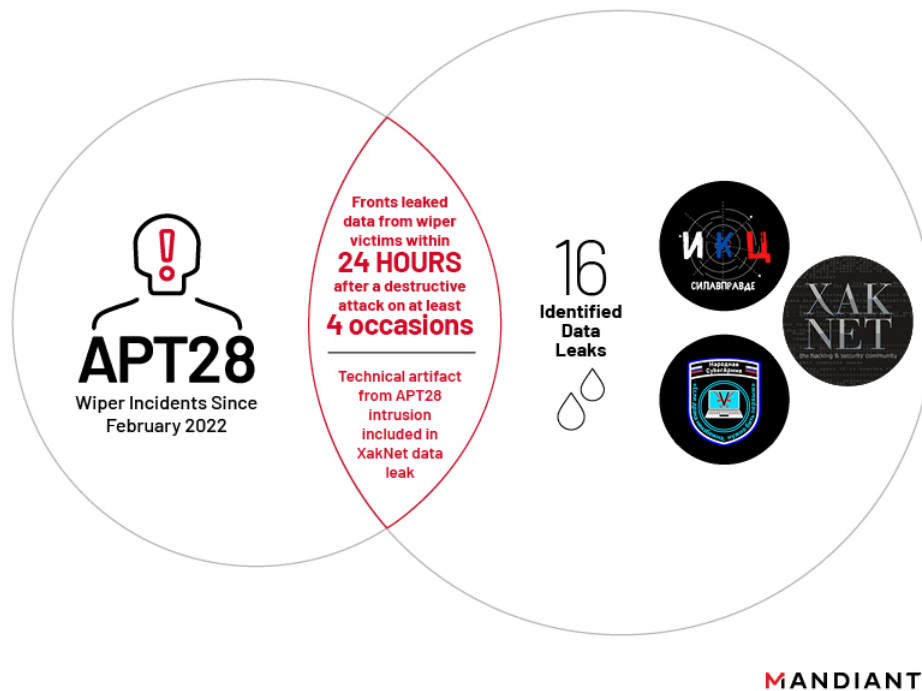


Figure 1: Suspected false hactivist fronts leaked data likely stolen from APT28 Wiper victims

### APT28 Wiped Ukrainian Victims Shortly Before Data Leaked on Social Media

We assess with moderate confidence that threat actors operating the Telegram channels XakNet Team, Infocentr, and CyberArmyofRussia\_Reborn are coordinating their operations with Russian Main Intelligence Directorate (GRU)-sponsored APT28. This assessment is based primarily on Mandiant's direct observations of the deployment of wipers used by APT28 on the networks of multiple Ukrainian organizations and the subsequent leaks of data by threat actors claiming to be hactivists likely originating from those entities on Telegram within 24 hours. We identified at least 16 data leaks from these groups, four of which coincided with wiping attacks by APT28.

- Mandiant has only observed the use of CADDYWIPER and ARGUEPATCH by APT28, although we note that others have publicly attributed some [CADDYWIPER](#) deployments to Sandworm.
- In two incidents, Mandiant observed APT28 conduct wiper attacks, which were followed, within 24 hours, by data from the victims being leaked on Telegram. In these instances APT28 deployed ARGUEPATCH ([22-00013040](#), [22-00009571](#)), which dropped the CADDYWIPER ([22-00006393](#), [22-00009571](#)).
- Two additional waves of CADDYWIPER attacks against multiple Ukrainian organizations were followed, within 24 hours, by data leaks from Ukrainian entities onto Telegram. In these cases, Mandiant cannot confirm that the organizations whose data was leaked were victims of the waves of coordinated wiper activity; however, the timing indicates that they were coordinated.
- In one XakNet data leak, Mandiant discovered a unique technical artifact from an APT28 intrusion. This indicates that APT28 had access to the same parts of the network from which the leak was sourced.

### XakNet Activity Consistent with Historical APT28 Information Operations

The three channels we identify in this report have claimed activity leveraging traditional hacktivist tactics, such as using distributed denial-of-service (DDoS) attacks, website defacements, and hack-and-leak activity to target their victims. Furthermore, XakNet's active solicitation of media coverage, in tandem with its self-promoted narrative of being a group comprised of Russian patriotic volunteers, suggests two possible influence objectives: the groups promote Russian interests abroad through their threat activity, and they promote the idea of average Russians supporting the government to domestic audiences through their claims to be patriotic volunteers amplified by the Russian media and elsewhere online.

The Russian intelligence services have an extensive history of using false hacktivist personas to support information operations and disruptive and destructive cyber activity. For example, this is a particularly well-established tactic of APT28 in activity targeting Ukraine and elsewhere, prominently including its use in the 2014 compromise, defacement, data leak, and destruction of the Ukrainian Central Election Commission's network and website, which was claimed by the pro-Russia "hacktivist" group [CyberBerkut](#). However, its most famous instance may be the [Guccifer 2.0 false persona](#) APT28 leveraged to interfere in the 2016 U.S. presidential election. U.S. Department of Justice [indictments](#) related to Russia's targeting of the 2016 U.S. presidential election have indicated that multiple GRU units were involved in that activity, including the unit to which APT28 is attributed (Unit 26165). We note this in recognition that it is possible multiple units within the GRU have likewise been involved in the activity outlined in this report.

Although we assess with moderate confidence that moderators respectively behind XakNet Team, Infocentr, and CyberArmyofRussia\_Reborn are at least coordinating with the GRU, we currently reserve judgement as to the composition of these groups and their exact degree of affiliation with the GRU. However, at a minimum, this coordination is consistent with frequent GRU tactics. While the exact nature of the relationship is unclear, it likely falls into one of two general possibilities:

- GRU officers directly control the infrastructure associated with these actors; their activities are a front for GRU operations, similar to the relationship between the GRU and the false persona Guccifer 2.0.
- The moderators running these Telegram channels directly coordinate with the GRU; however, the moderators are Russian citizens who are not Russian intelligence officers. There are multiple possible configurations through which this dynamic could manifest, including but not limited to initial GRU support for third parties to establish the channels or subsequent links established after initial channel creation.

A review of these channels' activity shows on-platform engagement by hundreds of users. In either of the above outlined scenarios, it seems likely that some or all of the users engaged with these channels are Russian-speaking civilians who are not intelligence officers. It is possible that the hundreds of users engaged with these channels are inauthentic, though we judge that to be unlikely.



Figure 2: XakNet Telegram post in which the group disputed previous public statements from Mandiant highlighting possible links between XakNet and the Russian Government. The third paragraph reads: "But in reality, everything is very simple. IB [information security] does not exist. Everything can be hacked. You can continue to conduct your super-cool investigations without any proof."

### **XakNet Team Moderators Likely Operate at Behest of the Kremlin**

"XakNet Team" is a Russian-language Telegram channel of a self-proclaimed hacktivist group that has conducted threat activity against Ukraine, including DDoS attacks, compromises and data leaks, and website defacements. The group claims to be comprised of Russian patriotic volunteers who formed the group in response to the Anonymous collective's declaration of war against Russia. The XakNet Team moderators advertise multiple domains and social media channels that we have determined are all controlled by the same group of threat actors. The XakNet Team moderators also claimed involvement in one of the more notable information operations observed so far in the conflict, when, in early March, a Ukrainian news organization's news ticker was defaced during a live TV broadcast with a fake message of Ukraine's capitulation to Russia attributed to President Zelenskyy ([22-00017141](#), [22-00007241](#)).

We assess with moderate confidence that the moderators of the XakNet Team channel are directly supported by APT28, based on XakNet's leak of a technical artifact APT28 employed during the compromise of a Ukrainian network. Given the unique nature of this technical artifact, we assess with moderate confidence that the moderators of XakNet Team either are GRU intelligence officers or work directly with the GRU APT28 operators conducting on-net operations.

- A Telegram channel was set up for the XakNet Team persona on March 1, 2022, and a Russian-language Wikipedia page for XakNet claims that "XakNet Team is a Russian group of hackers and hacktivists." Although the wiki page claims the group was created in February 2022 in response to the "cyberwar" declared by Anonymous against Russia, the edit history reveals that the wiki page was created on March 11 by a user with a Russia-based IP address (91[.]245[.]129[.]130) and no other Wikipedia contribution history. We have not attributed this IP address to a malicious threat actor, nor have we used it in our larger attribution assessment. However, we included this IP in our analysis as it made the early edits to this Wikipedia page.

- This likely represents an effort by the moderators to backstop the XakNet Team persona and make the false hacktivist front appear authentic. The wiki page is currently flagged for removal by Wikipedia moderators, one of which stated that the sources cited are "extremely dubious."
- We identified cached versions of the now-unavailable XakNet[.]team website and made the following observations:
  - The logo used on the XakNet[.]team website was the same as the one posted in the group's Telegram channel, a further indicator that the website was maintained by the same moderators (Figure 3). Images and text promoted on Telegram similarly were featured on the website when we viewed it.
  - The sidebar of the website links to the two Telegram channels we separately identified as linked to the same moderators, t[.]me/XakNet\_team and t[.]me/membersofXakNet[.]
  - On March 2, the day the website appeared, a post displayed on the homepage introduced the group, stating "XakNet is a team of Russian patriots who care about the fate of their native state," and asserting that "For every hack/ddos in our country, similar incidents will occur in Ukraine." This post is a further indicator of the group's alignment with and support for the Russian state, as well as the lengths that the group has gone to in order to define itself as "average" Russian citizens.
- Limited indicators, such as the existence of several seemingly unrelated online accounts carrying the XakNet name, suggest that the group may have coopted its name from an existing entity. Notably, XakNet has claimed lineage to a group that targeted Georgian entities during the Russia-Georgia War of 2008 through its use of their name.
- We have observed multiple instances in which XakNet Team and the other two Telegram channels have respectively either claimed to cooperate, engage in cross promotion, or otherwise seemingly align activity with each other. This type of activity is not unique to these three groups, though given other indicators outlined in this report, it could suggest possible inter-group links and highlight an imperative to further understand these dynamics in continued research.

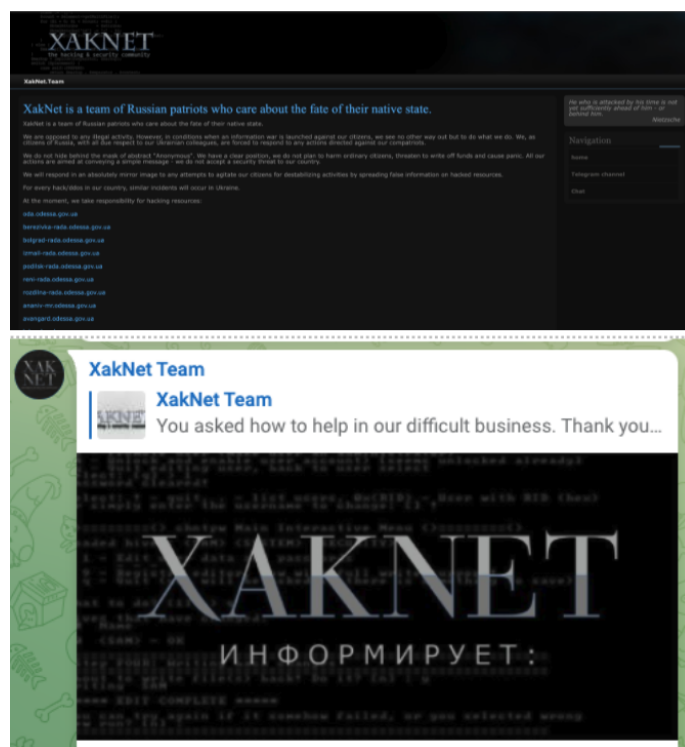


Figure 3: The same logo is used by the now-defunct domain (top image) and the identified Telegram channel (bottom image), a further indicator that both were run by the same actor.

CyberArmyofRussia\_Reborn is a Telegram channel Mandiant has tracked since mid-April 2022. Mandiant assesses with moderate confidence that the moderators of CyberArmyofRussia\_Reborn are at least coordinating with APT28 due to the timing of the leaks and the group's connection to XakNet, although the exact nature of the relationship is currently unclear. The channel's apparent goals include defamation, obtaining press, and influencing policy. CyberArmyofRussia\_Reborn moderators have leaked data from victims in at least the following industries: data services, local governments, and national governments, and the actors have claimed to degrade or deny services within a victim organization through DDoS or denial-of-service (DoS) attacks.

- In at least one-third of the data leaks Mandiant identified from CyberArmyofRussia\_Reborn, we directly or indirectly observed APT28 intrusion operations on the Ukrainian victim networks within 24 hours preceding the leaks.
- In several instances, we observed the moderators on this channel leak data in bulk including all files within a given extension or directory, and/or all files within a given date range. We identified the moderators leaking the following types of information from victims:
  - Files/personally identifiable information (PII)
  - General military documents
  - Domestic policies and documents

## DDoS с компьютера

### а) Инструкция по использованию скриптов (VPN не нужен)

На винде:

Для начала скачайте скрипт

Ссылка на скрипт: [https://t.me/CyberArmyofRussia\\_Reborn/71](https://t.me/CyberArmyofRussia_Reborn/71)

1) Запустите консоль из под администратора и перейдите в директорию со скриптом. Для этого:

I. Зайдите в пуск и введите в поиске cmd

II. Перейдите к расположению файла "Командная строка" и выполните

аналогичное действие в появившемся окне

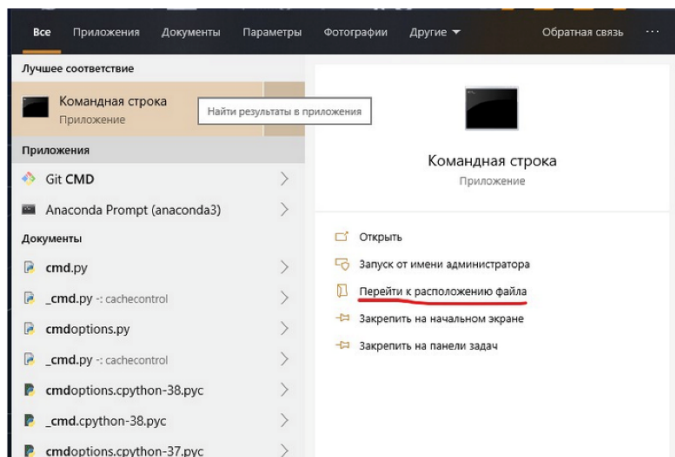


Figure 4: Screenshot of example instructions for running DDOS scripts on Windows provided to their members





Figure 5: New logo for the CyberArmyofRussia\_Reborn, the text of which reads "People's Cyber Army" with a quote notably used by Russia's President Putin: "If a fight is inevitable, you must strike first"

## Infocentr

On March 4, a Telegram channel for "Infocentr" was created, which appears to be dedicated to pro-Russia information operations and to fight against anti-Russian or pro-Ukrainian social media and other information channels. Mandiant assesses with moderate confidence that the moderators of the Infocentr channel are at least coordinating with APT28 due to the timing of the leaks and the group's connection to HakNet, although we have not yet determined the exact composition of the group. In at least one instance, HakNet reposted within a few minutes data that was initially leaked on the Infocentr Telegram page. It is possible this was a coincidence, but the close timing of the repost could indicate a closer relationship.

Приветствуем!

Всем вам уже давно понятно, какими способами Украина ведет войну как на земле, так и в информационном поле. Украина и Запад на полную развернули пропагандистскую машину по штамповке военных фейков и разжиганию ненависти к России и всему русскому.

Наблюдая данную картину, мы решили создать Информационно-координационный центр, который призван объединить неравнодушных граждан в борьбе с коричневой чумой 21 века.

**!** Мы просим оказать **любую** посильную помощь на информационном фронте!

🔍 Информационно-координационный центр ищет различных специалистов, готовых помочь в распространении достоверной информации о деятельности ВСУ и нацбатов и борьбе с укропропагандой в Телеграм и других социальных сетях.

Всех желающих присоединиться к нашему делу просим писать в бот [@iccenterbot](#).

Чем вы можете помочь Информационно-

Figure 6: Infocentr Telegram page in which the group introduces itself as an "Information and Coordination Center" and announces its operations against Ukraine and Western supporters

## Outlook

Mandiant is continuing to explore the relationship between the respective moderators of XakNet Team, Infocentr, and CyberArmyofRussia\_Reborn. Identifying the connections between so-called hacktivists and Russian espionage or attack groups can help victims assess risk when compromised, allow customers to prepare for the potential leak of their data, and potentially mitigate some effects. While we assess with moderate confidence that APT28 at least coordinates with the moderators of at least the three channels we identified in this report, potentially sharing or driving operations, it is also possible that the GRU or other Russian intelligence services are also coordinating with other self-professed hacktivist groups to target entities both within and surrounding Ukraine. As we continue to expand our knowledge of the actors behind recently emerged and long-standing channels such as KillNet, FromRussiaWithLove (FRWL), DeadNet, Beregini, JokerDNR (alternate spelling: JokerDPR), and RedHackersAlliance, Mandiant will continue to update our assessment on associations and drivers behind the actions and activities of these groups.

Vladimir Putin's obsession with returning Ukraine into the Russian sphere of influence created unprecedented circumstances for cyber threat activity ([22-00011952](#)). This likely is the first instance in which a major cyber power has conducted disruptive attacks, espionage, and information operations concurrently with widespread, kinetic military operations in a conventional war of force on force. We have never previously observed such a volume of cyberattacks, variety of threat actors, and coordination of effort within the same several months. We assess with high confidence that Russian cyber espionage and attack operations, while already a serious threat to Ukrainian organizations, pose an elevated risk to Ukraine as long as Russia continues its invasion.

**[Please rate this product by taking a short four question survey.](#)**

## First Version Publish Date

August 3, 2022 03:51:55 PM

### Threat Intelligence Tags

#### Actors

- APT28
  - Aliases
    - APT 28
    - APT-28
    - APT28

#### Affected Systems

- Users/Application and Software

#### Intended Effects

- Military Advantage
- Political Advantage
- Disruption
- Degradation



- Denial and Deception
- Embarrassment/Exposure/Brand Damage

## Motivations

- Ethnic/nationalist
- Military/Security/Diplomatic
- Ideological/Religious

## Malware Families

- ARGUEPATCH
  - Aliases
    - ARGUEPATCH
- CADDYWIPER
  - Aliases
    - CADDYWIPER

## Source Geographies

- Russia

## Tactics, Techniques And Procedures (TTPs)

- Malware Propagation and Deployment
- Distributed Denial-of-Service (DDoS) Attack
- Defacement

## Target Geographies

- Ukraine

## Targeted Information

- Government Information
- IT Information

## Version Information

Version:1, August 3, 2022 03:51:55 PM

This report contains content and links to content which are the property of Mandiant, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any Mandiant proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription.

©2022, Mandiant, Inc. All rights reserved.