Consejo Atlántico Juvenil Español
Spanish Youth Atlantic Treaty Association

News and Reports
www.coaje.es

Newsletter

September 2022

CYBERWARFARE: RUSSIAN HACKTIVIST AND NATION-STATE GROUPS IN THE RUSSO-UKRAINIAN WAR

Lucía Cuevas Díez

Abstract

The ongoing Russo-Ukrainian war has derived in unprecedent levels of malicious cyberactivity perpetrated by nation-state, cybercrime, and hacktivist groups. This article explains some basic concepts for understanding the role of the cybersphere in the conflict and summarizes some of the most relevant groups and actors involved in the Russian side of the conflict, including examples of cyberattacks carried out by them.

CYBERWARFARE: The Russo-Ukrainian war

Since the escalation of tensions between Russia and Ukraine began, multiple experts and researchers pointed out the possibility of witnessing a hybrid warfare that would incorporate cyberattacks as a weapon, especially on the Russian side. Although the impact and frequency of these expected have been moderated compared to expectations, cyber warfare has played – and still plays – a relevant and interesting role in the conflict. In this context, different types of cyberactivity have been

detected, associated to both nation-state and hacktivist threat groups. This article tries to summarize some of the main Russia-supporting threat actors and cyberattacks observed during the military conflict.

Within the cybersphere, we refer as **nation-state groups** to those threat groups that are linked to the government or military structure of a country, who finance them and guide their cyberactivity. The operations carried out by this type of groups are frequently aligned with the national interest of their country of origin. Although their objectives may vary, in most cases, nation-state groups perpetrate cyberattacks for obtaining intelligence (cyberespionage) or for disrupting the enemy – especially in a warfare context.

Several nation-state groups have been historically associated to the Russian state, among them:

- **APT28 (aka FancyBear, Tsar Team)** is a threat group attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165. This group has been active since at least 2004, targeting the Caucasus, Eastern Europe, NATO members, and European security and defense organizations.
- **APT29 (aka CozyBear, The Dukes)** is a threat group attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, targeting European and NATO member countries' government networks, as well as research institutes and think tanks.
- **Sandworm** is a threat group associated with the GRU's Main Center of Special Technologies (GTsST) military unit 74455, active since at least 2009. The group has targeted critical infrastructure organizations – from the government, energy, transport and finance sectors – for conducting cyber espionage and disruptive operations against NATO member states and Western countries.

Since the military conflict between Russia and Ukraine began, Russian government-backed groups have perpetrated several **cyberoperations** against Ukrainian and other targets, for instance:

- In March 2022, a cyberattack targeting satellite modems of the American company ViaSat disrupted internet services across Europe, also impacting Ukrainian military communications at the very beginning of the Russian invasion. The attack was attributed to the Russian threat group Sandworm.
- In February 2022, days before Russian troops invaded Ukraine, Russian government-backed threat actors distributed data-wiping malware to several Ukrainian institutions. This type of malware is aimed at destroying all the data of the infected system. At the same time, Russian threat actors ran misinformation campaigns targeting Ukrainian citizens, who received spam text messages claiming that ATMs were not working. Information operations aimed at spreading fake news related to the war have been very frequent during the last months.
- In April 2022, a new cyberattack was attributed to the Sandworm group. The operation targeted the energetic infrastructure of Ukraine, deploying two types of malware aimed at (i) disrupting activity, and (ii) eliminating evidence of the attack.

It is also worth mentioning that Russia has a long history of using its cyber capabilities against Ukraine. In June 2017, the Russian nation-state group Sandworm perpetrated one of the biggest cyberattacks against Ukrainian organizations. The attack affected multiple government, energy, and finance entities, causing losses of millions of dollars. The attack also affected

European organizations. This attack was conducted as part of a hybrid warfare between Russia and Ukraine following the 2014 conflict over Crimea.

Nevertheless, the ongoing military conflict between Russia and Ukraine has incorporated unprecedent levels of malicious cyberactivity perpetrated by a different type of threat actors/groups: **hacktivists**. Hacktivism is defined as the use of cybercrime techniques, malware, and other hacking tools to carry out an attack driven by ideological, religious, political, or moral motivations. The most prolific and famous hacktivist group is Anonymous, which operates globally against diverse targets based on political and moral motivations.

In the context of the Russo-Ukrainian (cyber)war, researchers have detected the emergence of numerous hacktivist and cybercrime groups who actively pledged support for Russia and the Russian government and showed willingness to conduct malicious cyberactivity against the enemy.

The **malicious cyberactivity** perpetrated by this type of groups shows a lower level of sophistication compared to nation-state groups. However, hacktivist groups have been observed deploying ransomware malware (provoking data encryption and activity disruption), perpetrating Distributed-Denial-of-Service (DDoS) attacks (flooding a website with a high number on requests so it stops responding), defacing websites (changing the content of a website, normally for showing political messages), claiming data breaches (leaking confidential information exfiltrated from the victims).

The total number of hacktivist-type threat groups/actors that have been involved in the cyberconflict derived from the Russo-Ukrainian war is unprecedented. These are some of the most notorious threat groups that remain active in the context of the conflict:

- **The CoomingProject**: threat group that extorts money from victims by exposing or threatening to expose leaked data. The threat group has stated its support to the Russian Government in response to cyberattacks against Russia.
- **Killnet**: threat group that strongly supports the actions of the Russian government, and that has perpetrated malicious cyberactivity – mainly DDoS and hacking – against Ukraine and other European and Western countries (e.g., Estonia, Lithuania, United States, Japan, among others).
- **XakNet**: Russian-speaking threat group that has been active as early as March 2022. The operators of the group have perpetrated DDoS attacks against multiple Ukrainian targets, as well as compromising the email of a Ukrainian government official. XakNet has collaborated with other pro-Russian hacktivist groups such as Killnet.

This article has summarized a small part of the recent and ongoing cyberactivity derived from the Russo-Ukrainian war, perpetrated by Russian or Russian-supporting threat actors. The unprecedented levels of cyberattacks, especially in the case of hacktivist-type of groups, may be a sign of a new trend in international conflicts. The information collected in this article reflects that cyberintelligence and cybersecurity are increasingly relevant fields of study within international security and defense, since it is expected to observe similar levels of activity in future conflicts.