FORESCOUT RESEARCH | VEDERE LABS

The Rise of State-Sponsored Hacktivism

An analysis of hacktivist attacks in 2024 and an outlook for 2025

Date: April 29, 2025

Contents

1. Executive Summary

At the end of 2022, we began reporting on hacktivist groups that align with nation-state interests in geopolitical conflicts. These groups expanded their tactics, techniques and procedures (TTPs) beyond website defacements and distributed-denial-of-service (DDoS) attacks towards sophisticated data leaks and disruption of cyber-physical systems within critical infrastructure.

Two years later, this trend has evolved. State-sponsored actors are adopting hacktivist personas to conduct cyberattacks driven by strategic factors, such as enhanced campaign visibility and plausible deniability for the perpetrators.

Critical infrastructure organizations are disproportionally targeted by hacktivists. Look at these key events:

- Between November 2023 and April 2024, at least 36 attacks targeted U.S. operational technology (OT) and industrial control systems (ICS).
- Most attacks focused on water utilities, however, healthcare, energy and manufacturing were also targeted.
- Key known players include:
    - CyberAv3ngers, who is believed to be affiliated with the Iranian military
    - Cyber Army of Russia, who is linked to Sandworm, a unit of the Russian GRU, launched attacks against U.S. water and wastewater facilities.

This report analyzes 780 hacktivist attacks in 2024 claimed by four groups operating on opposing sides of the Russia-Ukraine and Israel-Palestine conflicts: BlackJack, Handala Group, Indian Cyber Force, and NoName057(16).

KEY FINDINGS

WHAT YOU NEED TO KNOW

GROUPS / WHAT THEY TARGETED

NoName057(16) was by far the most active group, accounting for 90% of attacks.

These attacks targeted three primary asset types:

Websites: 91% of attacks

89% involved DDoS attacks that took websites offline

2% resulted in defacements

Data: 7% of attacks

7% led to data theft or leaks

Around **1%** resulted in data destruction

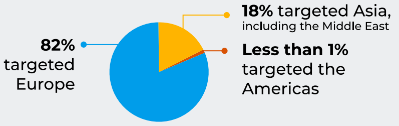
Routers, IoT, Other Devices/ Systems: 2% of attacks

WHERE THEY TARGETED

Hacktivist attacks spanned **40 countries**, including the most frequently targeted:

1. Ukraine (141 attacks)
2. Israel (80)
3. Spain (64)

Geographic distribution of attacks:



INDUSTRIES TARGETED

The top five affected industries are critical infrastructure sectors.

Government organizations: **44%**

Transportation and logistics: **21%**

Financial services: **13%**

Mitigation Recommendations: What You Need to Do

To counter hacktivist threats, organizations should implement the following security measures:

- Follow the NCSC-UK’s guide on Denial of Service attacks
- Harden IoT and OT security
- Strengthen network segmentation
- Enhance monitoring and threat detection

Read the entire “Conclusion and Mitigation Recommendations” section for full details.

2. The Rise of State-Sponsored Hacktivism

Hacktivism emerged in the 1990's as a form of digital activism that leveraged hacking techniques to advance social and political causes. Early hacktivists were often dismissed as "digital vandals", but their actions were primarily driven by anti-establishment ideologies including challenging authority, exposing corruption, opposing oppression, and advocating for freedom of information and speech. The most common techniques used by these early groups included website defacement and DDoS attacks. At the time, hacktivism was largely associated with grassroots activism and non-violent protest.

One of the most well-known hacktivist collectives, Anonymous, emerged in 2003, initially targeting governments and organizations it deemed oppressive. The group's decentralized structure and use of tactics, such as mass website takedowns and information leaks, exemplified the early hacktivist ethos.

Over time, hacktivism evolved. As political conflicts increasingly spilled into cyberspace – and vice-versa – hacktivist groups shifted from loosely coordinated collectives to sophisticated, structured organizations with nationalistic motivations. Since the 2010s, many hacktivist groups have maintained the façade of grassroots activism while actively serving nation-state interests.

Modern hacktivism now differs significantly from its origins. Instead of solely advocating for ideological causes, today's hacktivists frequently target adversarial critical infrastructure and manipulate public opinion to advance the strategic objectives of nation-states. This transformation has blurred the lines between traditional hacktivism and state-sponsored cyber operations, making it increasingly difficult to distinguish between independent activists and proxy actors working on behalf of governments

Hacktivist activity has surged since the escalations of the Russia-Ukraine and Israel-Palestine conflicts in 2022 and 2023, respectively. These conflicts have created an ideal environment for nationalistic hacktivist groups to amplify their agendas in cyberspace. Several key factors have contributed to this increase, making it easier and more effective for hacktivist groups to engage in cyber campaigns:

- **Polarized global opinion fuels recruitment and engagement**
  The deep ideological divide surrounding both conflicts has intensified public attention, providing hacktivist groups on opposing sides with greater visibility and a steady influx of followers or recruits.

- **Hacktivism plays a growing role in information warfare**
  Cyber campaigns have become a critical tool for controlling narratives and shaping public perception. Even less sophisticated attacks – such as website defacements and data leaks - can manipulate public opinion, discredit adversaries, and erode trust in institutions.

- **Increased access to offensive cyber tools**
  The tools needed to conduct cyberattacks, including targeting critical infrastructure and operational technology, are now more widely available to both individuals and groups. This accessibility has lowered the barrier to entry for hacktivists, allowing them to launch disruptive attacks with minimal technical expertise.

Alongside the rise of nationalistic hacktivism, two significant trends have emerged:

- **State-sponsored hacktivism**
  Some governments actively support hacktivist groups, either directly - by providing tools, intelligence on targets, and financial resources - or indirectly, by shielding them from prosecution or recognizing and rewarding their achievements.

- **"Faketivism" – the state masquerading as hacktivists**
  Though less commonly discussed than state-sponsored hacktivism, faketivism refers to government agencies or state-affiliated actors that adopt the branding, tactics, and imagery of grassroots hacktivist groups. These entities operate under the guise of independent hacktivists but are, in reality, directly employed by national governments or state-linked corporations to promote government-aligned narratives and conduct cyber operations.

A notable early example is "Predatory Sparrow," a group that presents itself as a dissident force opposing the Iranian government, but is widely believed to be affiliated with Israel. Similarly, Iranian groups such as "Karma Power" and "The Malek Team" have conducted cyberattacks on Israeli critical infrastructure and are suspected of ties to Iran's Ministry of Intelligence or the Islamic Revolutionary Guard Corps (IRGC).

This evolution has transformed hacktivism into an offensive cyber weapon used by states both directly and indirectly for cyber espionage, disinformation campaigns, and critical infrastructure attacks. These trends demonstrate how hacktivism has evolved beyond grassroots activism into a core component of "hybrid warfare" where cyberattacks, disinformation campaigns, and geopolitical influence operations are deeply interconnected.

This weaponization of hacktivism offers several key advantages to nation states, making it a valuable tool for cyber warfare and information operations because of:

- **Plausible deniability.** Governments can distance themselves from the activities of hacktivist groups by claiming they have no direct control over their actions. This allows nation-states to conduct cyber operations without overtly violating international norms or risking diplomatic consequences.

- **Attribution challenges.** Cyberattack attribution is notoriously difficult, but when independent hacktivists, state-sponsored groups, and faketivists collaborate - as they increasingly do - it becomes even harder to distinguish between them or attribute their actions to real-world individuals or groups. This ambiguity complicates response strategies allowing state-backed actors to operate with greater impunity.

- **Illusion of public support.** The hacktivist persona adopted by state-sponsored groups can create the impression of widespread grassroots support for a government's actions. This makes it appear as if a large number of independent individuals are voluntarily rallying behind a nationalistic cause, reinforcing state propaganda.

- **Exaggerated or fabricated impact.** Hacktivists often sensationalize their attacks, exaggerating their success or even fabricating cyber incidents. State actors can exploit this tactic, using hacktivist-style language and imagery to amplify the perceived impact of their operations. When combined with disinformation strategies - such as AI-generated images designed to evoke strong emotional reactions - this manipulation can reshape public perception of an event or a target, furthering strategic objectives.

By leveraging these advantages, nation-states have transformed hacktivism into a sophisticated tool of hybrid warfare.

3. Overview of Groups and Attacks

With hacktivism increasingly intertwined with state interests, understanding the operational tactics of the most active groups provides insight into modern cyber conflict. To examine these dynamics, we analyzed the activities of four highly active and influential hacktivist groups from January until October 2024. These groups, listed alphabetically, represent different geopolitical alignments and operational tactics:

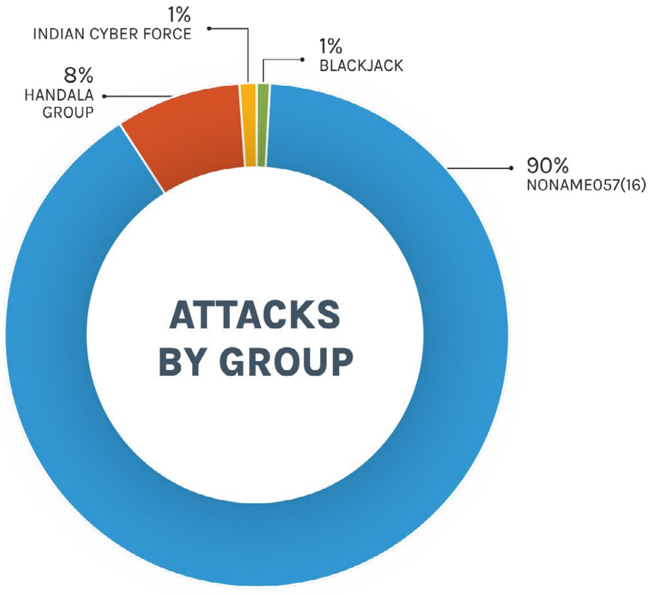
- **BlackJack**, a Ukrainian group active since October 2023 is known for targeting Russian companies and critical infrastructure. Their activities primarily involve breaching databases, exfiltrating sensitive information, publishing stolen data and, in some cases, wiping records entirely. Unlike other groups, BlackJack maintains a relatively low-profile presence on Telegram, where they occasionally claim responsibility for their attacks. The group is believed to have affiliations with Ukrainian intelligence services.

- **Handala Group**, an Iranian group that emerged in December 2023, specializes on a wide range of cyber operations, including phishing, ransomware, website defacement, data theft, and extortion. Their attacks predominantly target Israeli organizations, aligning with their strongly pro-Palestine stance. Handala Group actively publicizes its operations through a dedicated Telegram channel and an official website, leveraging these platforms to claim responsibility and amplify its messaging.

- **Indian Cyber Force**, an Indian hacktivist group active since December 2022, focuses on cyberattacks against critical infrastructure in nations that oppose its pro-India and pro-Israel viewpoints. The group engages in aggressive online activity, frequently using social media platforms like X and Telegram to claim responsibility for its attacks and interact with its followers.

- **NoName057(16)**, a Russian hacktivist group active since March 2022, is best known for its large-scale DDoS attacks against organizations in Ukraine and nations that support Ukraine. This group maintains the most active Telegram presence among the four, posting multiple daily updates about its attacks. By consistently tracking and promoting its operations online, NoName057(16) has positioned itself as one of the most visible and persistent hacktivist entities in the ongoing cyber conflict.

To analyze the activities of these hacktivist groups, we monitored their Telegram channels, X accounts and other media platforms, compiling a dataset of 780 claimed attacks. As shown in Figure 1. NoName057(16) was by far the most active group, responsible for 704 attacks, accounting for 90% of all recorded incidents.



Source: Forescout Research Vedere Labs

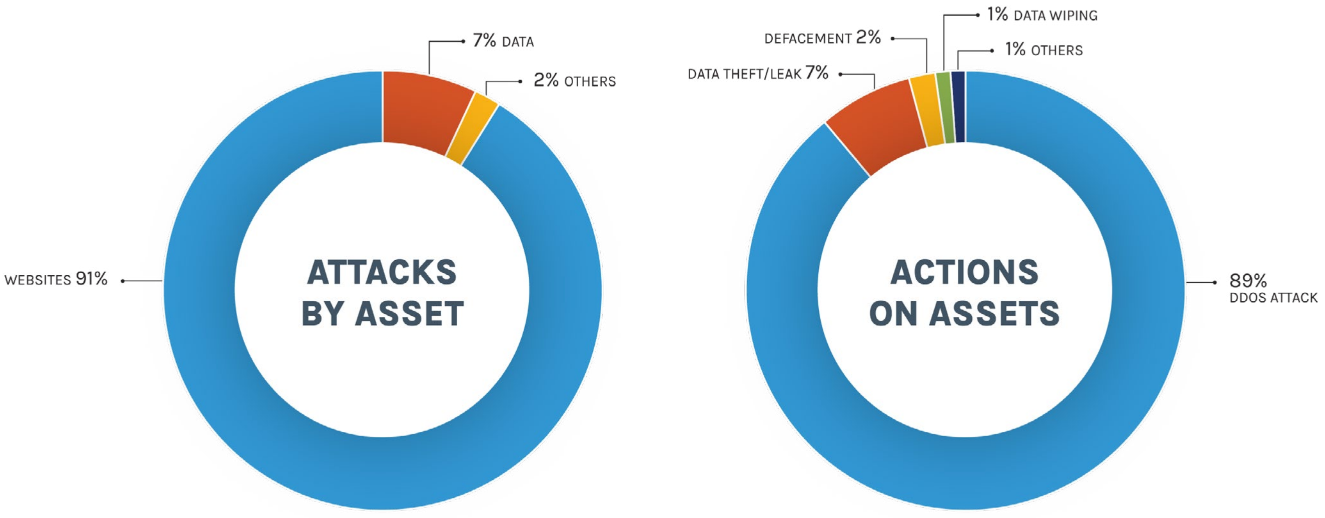
Figure 1 – Attacks by hacktivist group

These groups primarily targeted three categories of assets, as illustrated in Figure 2.

- **Websites (91% of attacks)**
  - 89% of attacks involved DDoS, taking websites offline
  - 2% of attacks resulted in website defacement.

- **Data (7% of attacks)**,
  - 7% of attacks led to data theft or leakage
  - Around 1% of attacks involved data being wiped.

- **Other assets such as routers and IoT devices (2% of attacks)**
  - Methods included malware installation, data encryption on devices, tampering with device configurations and forced shutdowns.



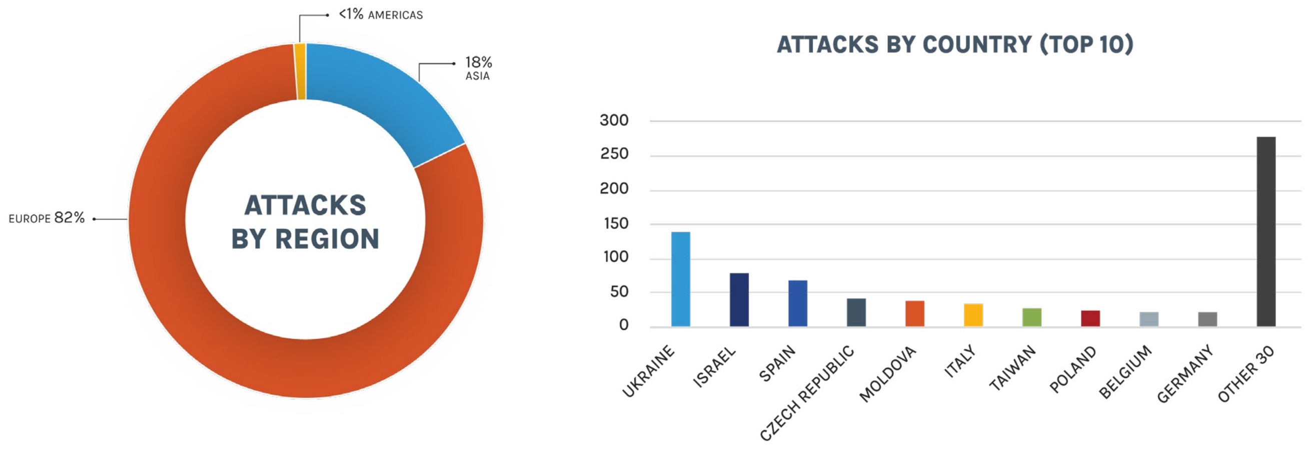
Source: Forescout Research Vedere Labs

Figure 2 – Attacks by asset and actions on asset

As illustrated in Figure 3, the majority of hacktivist attacks were concentrated in Europe and Asia, reflecting the geopolitical alignments of the groups involved.

- **82% of attacks targeted Europe, while 18% focused on Asia (including the Middle East)**. Less than 1% of attacks were directed at the Americas. This distribution aligns with the strategic objectives of the hacktivist groups, as those aligned with Russia primarily target European countries supporting Ukraine, while groups aligned with Palestine focus on Israeli entities, among other region-specific patterns.

- In total, 40 countries were attacked. The most targeted nations were Ukraine (141 attacks), Israel (80 attacks) and Spain (64 attacks).

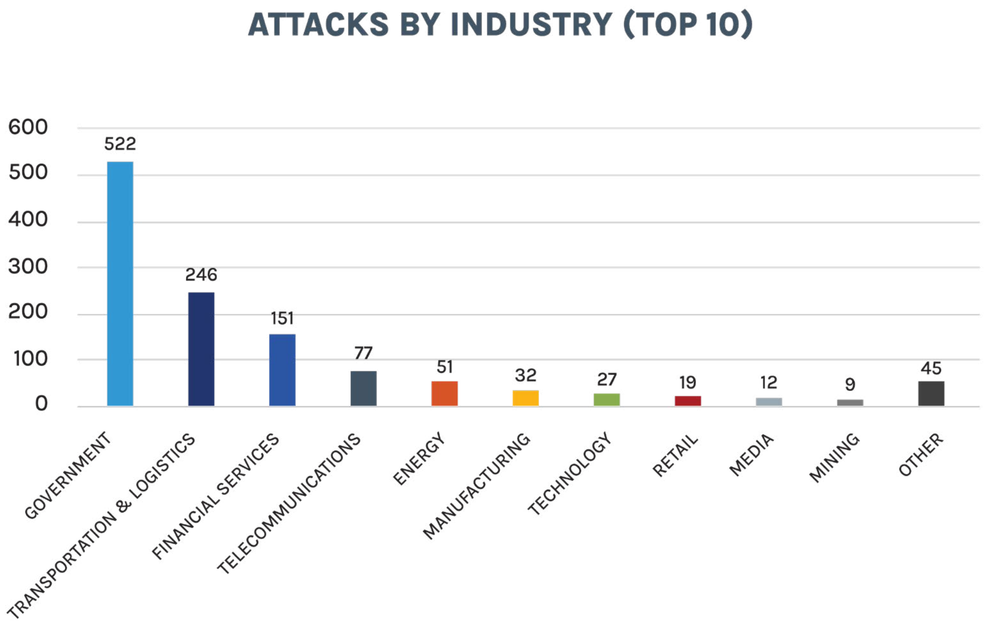


Source: Forescout Research Vedere Labs

Figure 3 – Attacks by region and country

As illustrated in Figure 4, the majority of hacktivist attacks targeted critical infrastructure sectors, with the top three industries accounting for over 75% of all incidents.

- 44% of targeted entities were governmental organizations including military services.
- 21% of attacks focused on the transportation and logistics sector, with key targets including ports, airports, roads, railways and urban transportation systems.
- 13% of attacks targeted financial services companies, disrupting banking, payment systems, and other financial infrastructure.
- All of the top five industries targeted are critical infrastructure sectors.



Source: Forescout Research Vedere Labs

Figure 4 – Attacks by industry

The concentration of attacks on critical infrastructure sectors highlights how hacktivist campaigns are not merely symbolic but strategically designed to disrupt essential services, erode public trust, and apply geopolitical pressure.

4. Analysis of Groups and Attacks

1. BlackJack

Table 2 outlines BlackJack's operations during the study period, showing that all of their targets were located in Russia. The group attacked organizations across a diverse range of industries, including broadcasting, internet providers, education, banking, electrical engineering, and government.

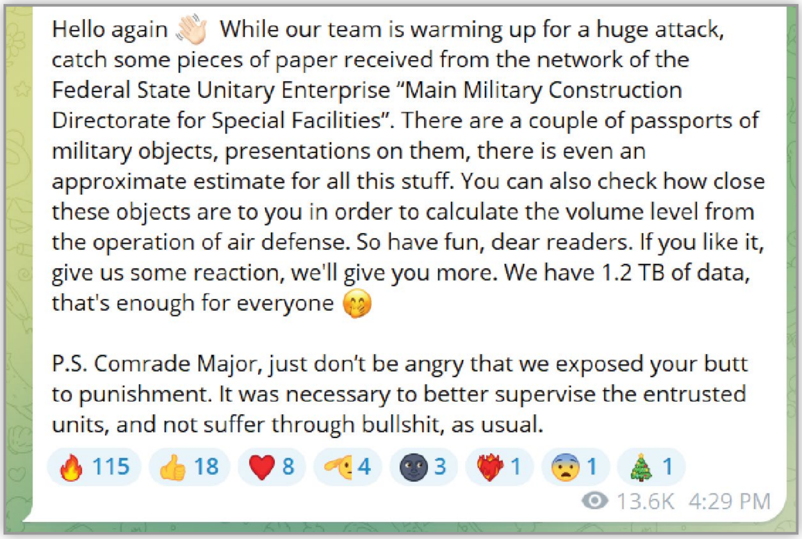
The majority of BlackJack's attacks involved data theft, although there were also instances of data wiping, demonstrating an intent not only to exfiltrate sensitive information but also to disrupt operations. Beyond compromising data, the group targeted various devices, including broadcast servers, hypervisors and routers. Their most notorious attack leveraged custom-made malware to disrupt sewage systems in Moscow, a case examined in more detail below.

Table 1 – BlackJack targets

Date	Targeted organizations (with link to reference)
Jan 1	Siberian Bear IPTV broadcast server
Jan 8	M9com internet provider
Jan 18	Federal State Unitary Enterprise "Main Military Construction Directorate for Special Facilities"
Feb 13	St. Petersburg State University
Mar 18	"First Line" internet provider (LLC "High Technologies")
Apr 8	OWEN holding company
Apr 9	JSC Moskollektor
Jun 24	PJSC "Agregat"
Jul 11	Kazan electrotechnical plant

Two of BlackJack's attacks received widespread media attention, demonstrating the group's capability to exfiltrate and disrupt critical Russian assets.

- On January 18, as illustrated in Figure 5, BlackJack claimed responsibility for stealing 1.2 terabytes of data from a Russian state enterprise involved in construction for Russia's military - the Federal State Unitary Enterprise "Main Military Construction Directorate for Special Facilities". The stolen data reportedly included maps of Russian military bases within Russia and occupied Ukraine, as well as classified information on Russian military weapon storage, air defense installations, and command-and-control infrastructure. Beyond data theft, BlackJack wiped information from seven Russian servers and encrypted or disabled hundreds of computers belonging to Russian military contractors, effectively crippling operations and causing significant disruption.

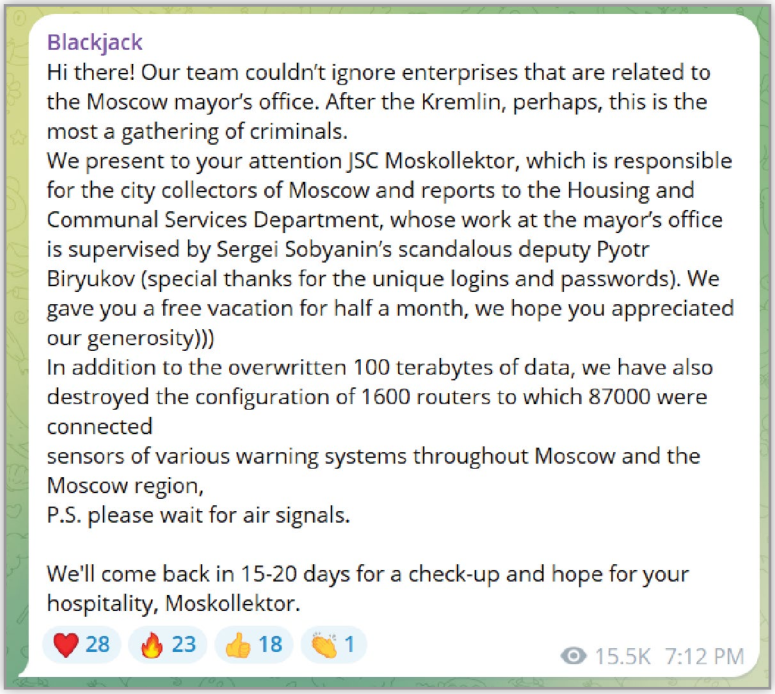


Hello again 👋 While our team is warming up for a huge attack, catch some pieces of paper received from the network of the Federal State Unitary Enterprise "Main Military Construction Directorate for Special Facilities". There are a couple of passports of military objects, presentations on them, there is even an approximate estimate for all this stuff. You can also check how close these objects are to you in order to calculate the volume level from the operation of air defense. So have fun, dear readers. If you like it, give us some reaction, we'll give you more. We have 1.2 TB of data, that's enough for everyone 🤭

P.S. Comrade Major, just don't be angry that we exposed your butt to punishment. It was necessary to better supervise the entrusted units, and not suffer through bullshit, as usual.

Figure 5 - BlackJack Telegram post about their attack on the Russian Federal State Unitary Enterprise

- On April 9, as illustrated in Figure 6, BlackJack claimed responsibility for an attack on Moscollector, a Russian company responsible for sewage, water, and communications infrastructure. The group reportedly deployed a novel OT/ICS malware named "Fuxnet" to target Moscollector's network operations center and disable 87,000 AO SBK sensors. BlackJack described Fuxnet as "Stuxnet on steroids," suggesting an advanced disruptive capability specifically designed for industrial control systems The malware carried out multiple destructive actions, including deleting critical files and routing table information, disabling remote access services and rewriting the flash memory of the sensors. BlackJack also claimed to have overwritten 100 terabytes of data and destroying the configuration of 1,600 routers.



Blackjack
Hi there! Our team couldn't ignore enterprises that are related to the Moscow mayor's office. After the Kremlin, perhaps, this is the most a gathering of criminals.
We present to your attention JSC Moskollektor, which is responsible for the city collectors of Moscow and reports to the Housing and Communal Services Department, whose work at the mayor's office is supervised by Sergei Sobyanin's scandalous deputy Pyotr Biryukov (special thanks for the unique logins and passwords). We gave you a free vacation for half a month, we hope you appreciated our generosity)))
In addition to the overwritten 100 terabytes of data, we have also destroyed the configuration of 1600 routers to which 87000 were connected
sensors of various warning systems throughout Moscow and the Moscow region,
P.S. please wait for air signals.

We'll come back in 15-20 days for a check-up and hope for your hospitality, Moskollektor.

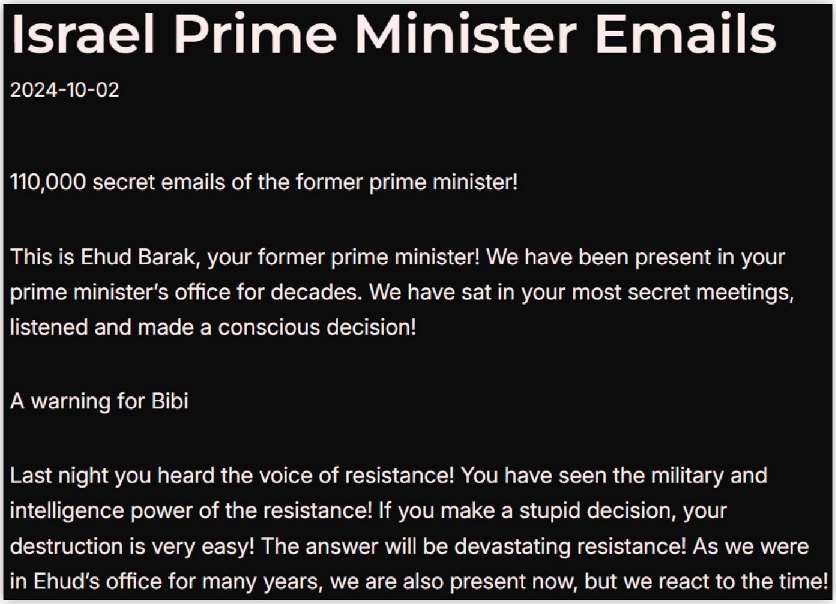
Figure 6 - BlackJack Telegram post about their attack on Moscollector

Given BlackJack's suspected affiliation with Ukrainian intelligence services, these attacks exemplify the rise of state-sponsored hacktivism - or arguably state hacking - which has become a key component of the cyber dimension of the Russia-Ukraine conflict.

2. Handala Group

Handala Group exclusively targeted Israeli organizations across a wide range of industries, including transportation, healthcare, technology, agriculture, engineering, textile, government, and education. Their primary attack methods involved data leaks, with some instances of ransomware deployment. Devices targeted included phones, radar systems and broadcast servers.

A key focus of Handala Group has been leaking data claimed to belong to high-level government officials, as illustrated in Figure 7. These leaks are often designed to embarrass the targeted officials while eroding public confidence in the government's ability to secure sensitive information. By weaponizing data exposure, Handala Group amplifies the psychological and political impact of its cyber operations.



Israel Prime Minister Emails

2024-10-02

110,000 secret emails of the former prime minister!

This is Ehud Barak, your former prime minister! We have been present in your prime minister's office for decades. We have sat in your most secret meetings, listened and made a conscious decision!

A warning for Bibi

Last night you heard the voice of resistance! You have seen the military and intelligence power of the resistance! If you make a stupid decision, your destruction is very easy! The answer will be devastating resistance! As we were in Ehud's office for many years, we are also present now, but we react to the time!

Figure 7 – Handala Group's webpage claiming an attack on Ehud Barak's Emails

Two of Handala Group's attacks in 2024 gained widespread media attention, showcasing their ability to compromise critical systems and use cyberattacks as a tool for political retaliation.

- On April 14, the group claimed to have breached the Israeli radar system and sent threatening messages to 500,000 Israeli citizens. This attack not only targeted military infrastructure but also sought to instill fear among the civilian population, highlighting Handala's use of cyber operations for psychological warfare.
- In September, the group launched attacks on two organizations, which they framed as retaliation for the tampering of batteries that caused Hezbollah's pagers to explode. Their first target was Vidisco, a company responsible for manufacturing X-ray scanners used by over 84% of air and seaports worldwide. Handala Group claimed to have discovered a backdoor in Vidisco's scanners that allowed the explosives used in the pager attacks to go undetected until they reached Lebanon. In a second attack, they breached Israeli Industrial Batteries (IIB), the company they alleged was responsible for producing the explosives used in the pagers. During this breach, the group stole 14 terabytes of data, which they threatened to leak.

Handala Group stands out among the hacktivist organizations studied due to its dedicated webpage for publicizing attacks. Several factors likely motivated this decision. A self-hosted website grants greater control over content free from moderation or deletion by platform administrators. It also ensures longer-lasting visibility of their posts, particularly since their Telegram channels have frequently been taken down. Additionally, a professional-looking webpage enhances the group's credibility, positioning them as an organized operation rather than a fringe entity, ultimately attracting a broader audience beyond niche Telegram communities.

3. Indian Cyber Force

Table 2 details the Indian Cyber Force's operations during the study period, showing a diverse range of geopolitical motivations behind their attacks. The group's targets were located in several countries, reflecting both historical tensions and recent political conflicts:

- Pakistan was the most targeted country, with attacks largely justified as a response to ongoing political tensions and conflicts. The group frequently referenced the 2019 Pulwama attack, using it as a rallying point for their cyber operations. The historical rivalry between India and Pakistan, dating back to their partition in 1947, played a key role in their aggressive targeting of Pakistani entities.
- Indonesia was also targeted as a part of the group's commemoration of the Pulwama attack.
- The Maldives became a focus following recent diplomatic tensions, where statements made by the Maldivian government were interpreted as inflammatory and offensive, prompting retaliatory cyberattacks.
- Canada and the United Kingdom, were targeted specifically for their Muslim organizations, suggesting a religiously motivated aspect to some of the group's activities.
- Bangladesh was attacked due to ongoing tensions between the two nations.

Indian Cyber Force's targeted sectors spanned travel, education, marketing, aviation, banking, law enforcement, and government. The majority of their attacks involved website defacement, aiming to publicly humiliate and disrupt their targets, while a smaller number of incidents involved data theft and leaks.

Table 2 – Indian Cyber Force targets

Date	Targeted organizations (with link to reference)	Country
Jan 15	Blue Horizon Maldives Travel Agency	Maldives
Jan 26	Online Quran Teacher BD	N/A
Feb 13	Leaders' Odyssey School and College, PVMC, Teknik Informatica UMAHA, JSMarketing, Galveston Aviation Services	Pakistan, Indonesia
Feb 14	HBL Bank	Pakistan
Feb 14	Pakistan Sindh Police	Pakistan
Feb 14	Pakbanks, 11thclassresult, Hamzzzinterior, Armanapparels, Countrygroup, e-nikahservice, Molekulzinternational, Watermatsports, attarigadgets, Clickmag	Pakistan
Jun 19	More than 80 (mainly retailers)	Pakistan, Canada, United Kingdom
Jun 19	National Bank of Pakistan Surveillance, Zeenwoman Surveillance, ATMs, power plants, shopping malls, mosques, post offices, other private organizations	Pakistan
Aug 12	Grameenphone	Pakistan
Aug 17	Government of Bangladesh National E-Mail System, government and nongovernment websites	Bangladesh

The group primarily focused on website defacements, emphasizing symbolism, visibility, and influence rather than technical sophistication. While defacements are not highly advanced cyberattacks, they serve a crucial psychological and propaganda function, allowing the group to assert its presence in cyberspace and publicly demonstrate its ability to breach targeted systems.

Their second most common attack method involved data theft and leaks, particularly targeting banks and governmental institutions. By exposing sensitive financial and state-related information, these attacks aimed to undermine institutional credibility and escalate geopolitical tensions.

Beyond defacements and data breaches, the group also hacked surveillance cameras in a variety of locations, including banks, ATMs, power plants, malls, mosques, post offices, and other private organizations. These intrusions, while less publicized than their website defacements, suggest an intent to compromise security infrastructure and gather intelligence on high-profile targets.

4. NoName057(16)

NoName057(16) conducted cyberattacks against private corporations and public institutions in Ukraine and countries supporting Ukraine, targeting organizations across Europe, Asia, and North America. However, the group demonstrated a clear preference for European NATO members, frequently launching attacks against institutions within these nations.

Unlike other hacktivist groups that exhibit selective targeting strategies, NoName057(16) adopted a broad and high-frequency attack approach, often carrying out multiple attacks a day across different industries and countries. Some attacks targeted the same organizations repeatedly, either due to their strategic value or to demonstrate the group's continued ability to inflict damage. At times, the group narrowed its focus to specific sectors within a country, dedicating days or more to targeting entities such as the Ukrainian energy sector, Polish logistics companies, or governmental institutions in Nordic countries.

The vast majority of their attacks targeted websites via DDoS. NoName057(16) has been an active participant in the DDoSia project, a large-scale pro-Russian DDoS initiative launched in August 2022 in collaboration with allied hacktivist groups. The project provides attackers with a DDoS attack toolkit, which is considered the successor to the Bobik botnet and is used extensively against Ukrainian and NATO-aligned targets.

NoName057(16) actively recruits and mobilizes supporters via its Telegram channel, encouraging individuals to download DDoSia tools and join cyberattacks against so-called 'Russophobic' states. Participation is incentivized not only ideologically but also financially, as volunteers who execute successful DDoS attacks receive monetary rewards.

While NoName057(16)'s direct ties to the Russian government remain unconfirmed, previous research has identified connections between the group and the Cyber Army of Russia Reborn (CARR). CARR in turn is known to be a front for the Sandworm APT, a well-documented Russian state-sponsored cyber unit known for its advanced cyber warfare capabilities.

5. Conclusion and Mitigation Recommendations

This report examined the evolution of hacktivism, tracing its transformation from grassroots activism to a tool of state-aligned and state-sponsored cyber operations. By analyzing four highly active hacktivist groups in 2024. We explored their motivations, targeting patterns and attack methods, illustrating how geopolitical conflicts increasingly shape cyber threats.

The ongoing conflicts in Europe and the Middle East have fueled the rise of hacktivist groups with direct or indirect ties to state actors. The U.S. Homeland Threat Assessment 2025 predicts that *“criminal hacktivists sympathetic to Russia will continue to carry out disruptive cyber attacks against poorly protected Western critical infrastructure to weaken US resolve in supporting Ukraine.”*

We agree with this assessment and extend it with the following expectations for 2025:

- **DDoS will remain the primary attack method**. DDoS attacks are the easiest to execute, especially with tools like NoName057(16)’s DDoSia, which can be quickly downloaded and deployed by supporters. This accessibility ensures that DDoS remains the go-to tactic for hacktivist groups.

- **Attacks on IoT and OT systems will increase**. While DDoS attacks gain visibility, attacks directly targeting IoT and OT devices - such as BlackJack’s Fuxnet malware – attract even more attention due to their potential for cyber-physical disruption. As these attacks grow more frequent, technical knowledge about OT vulnerabilities will continue spreading among hacktivist groups a trend we previously documented when hacking guides for Unitronics PLCs circulated on Telegram channels.

- **Critical infrastructure will remain the primary target**. Our 2024 threat roundup identified critical infrastructure sectors as the top target of cyberattacks, and that trend holds for hacktivist campaigns as well. Hacktivists focus on industries that have an immediate impact on daily life, such as financial services and government entities. While DDoS and data exfiltration will dominate attacks on financial services and government entities, IoT and OT exploitation will be the preferred method for disrupting sectors heavily reliant on connected devices, as seen in ongoing attacks against water utilities.

- **Hacktivists will prioritize active conflict zones**. The highest volume of attacks has targeted countries in active conflict (e.g. Ukraine and Israel) or nations openly supporting them (e.g. the U.S. and European allies). As conflicts evolve, hacktivist groups will adjust their targeting based on geopolitical shifts, such as ceasefires, peace deals, or the escalation of other tensions into full-scale wars.

- **More governments will adopt hacktivist personas**. Russia, Ukraine, Iran, and Israel have already leveraged hacktivist fronts for cyber operations. As new conflicts emerge, more states are expected to deploy hacktivist proxies, or expand support for ideologically aligned groups, to carry out cyberattacks, with plausible deniability.

- **Hacktivist groups and identities will shift over time**. While hacktivist groups thrive on notoriety, high visibility also attracts the attention of other governments and law enforcement, leading to sanctions, indictments, or countermeasures. Like ransomware gangs, which frequently rebrand or fragment to avoid legal consequences, hacktivist organizations are likely to adopt similar tactics - splitting into smaller factions or re-emerging under new identities to continue operations.

To counter current and future hacktivist threats, organizations should implement the following security measures:

- **Follow the NCSC-UK's guide on Denial of Service attacks, which includes:**
  - Identifying weak points in your service infrastructure
  - Ensuring that service providers can handle resource exhaustion scenarios
  - Scaling the service to withstand concurrent attack traffic
  - Developing a response plan and conducting regular stress testing.

- **Harden IoT and OT security.**
  - Identify and patch vulnerabilities in IoT/OT devices
  - Change default or easily guessable passwords on all IoT/OT systems.
  - Avoid exposing IoT/OT devices directly to the internet - instead follow CISA's best practices for providing remote access for industrial control systems.

- **Strengthen network segmentation**
  - Isolate IT, IoT, and OT networks to prevent lateral movement in case of a breach.

- **Enhance monitoring and threat detection**
  - Continuously monitor IoT/OT network traffic to detect anomalies and identify devices being co-opted into botnets or DDoS campaigns.