# State-sponsored hacktivism escalates in 2024, targeting critical infrastructure across conflict zones



In an extensive analysis conducted by Forescout Technologies Inc., the cyber threat landscape shaped by hacktivist groups in 2024 has been comprehensively examined, revealing significant patterns and shifts in the nature of cyber conflicts tied to geopolitical tensions. The report titled ‘The Rise of State-Sponsored Hacktivism: An analysis of hacktivist attacks in 2024 and an outlook for 2025’ sheds light on how hacktivism, once rooted primarily in ideological activism, has transformed into a strategic instrument within state-aligned conflicts, particularly in the contexts of the Russia-Ukraine and Israel-Palestine disputes.

Between November 2023 and April 2024, Forescout documented around 780 hacktivist attacks conducted by groups including BlackJack, Handala Group, Indian Cyber Force, and NoName057(16). These groups are affiliated with or supportive of the factions engaged in the aforementioned conflicts, targeting critical infrastructure across multiple sectors. Government and military systems constituted the primary targets, accounting for 44% of attacks, followed by transportation and logistics with 21%, and financial services making up 13%. Other sectors such as telecommunications, energy, and manufacturing were also frequently targeted, underscoring the broad strategic intent behind these campaigns.

Most attacks—91%—were aimed at websites, with Distributed Denial of Service (DDoS) attacks comprising 89% of this category, rendering sites inaccessible and disrupting services. Defacement, data theft, and data wiping formed smaller but notable portions of activity. According to the report, these campaigns predominantly unfolded across Europe and Asia, with 82% of attacks directed at European nations, especially Ukraine, which endured 141 incidents. Israel and Spain also experienced high levels of cyber aggression, logging 80 and 64 attacks respectively.

The report highlights the evolution of hacktivism from independent grassroots endeavours to sophisticated, state-influenced operations blurring the lines between genuine activism and proxy cyber warfare. Forescout identified notable players such as CyberAv3ngers, believed to be linked to the Iranian military, and the Cyber Army of Russia, associated with Sandworm, the cyber unit of the Russian GRU, which executed attacks on US water and wastewater facilities. These incidents indicate an increasing focus on operational technology (OT) and industrial control systems (ICS), with at least 36 attacks recorded on US critical infrastructure sectors during the study period.

Forescout emphasises that hacktivism serves multiple strategic purposes in modern conflicts, including espionage, disinformation, and disruption. The accessibility of cyberattack tools has lowered barriers, allowing actors with minimal technical expertise to conduct impactful operations. The report cites groups like Predatory Sparrow, reputedly linked to Israel, and Iranian-aligned groups such as Karma Power and The Malek Team, targeting respective adversaries’ critical infrastructure in a tit-for-tat cycle indicative of hybrid warfare tactics.

Several prominent hacktivist groups were analysed in detail:

* BlackJack, active since October 2023, primarily targets Russian entities with database breaches and data destruction, maintaining a low profile but believed to have connections to Ukrainian intelligence.
* Handala Group, formed in December 2023, is an Iranian pro-Palestinian collective known for ransomware, data leaks, and psychological operations, targeting Israeli transportation, healthcare, technology, and government sectors. Their use of a professional website for publicity and data leaks distinguishes them within the hacktivist community.
* Indian Cyber Force, initiated in December 2022, shows a pro-India and pro-Israel stance, conducting widespread attacks against nations like Pakistan, Indonesia, and Bangladesh. Their focus includes website defacements and sensitive data theft, often tied to historical and geopolitical grievances.
* NoName057(16), a prolific Russian group dating back to March 2022, is heavily engaged in high-volume DDoS attacks targeting Ukraine and its allies, operating openly on social media while linked to Russian military cyber units through the Cyber Army of Russia Reborn.

BlackJack, active since October 2023, primarily targets Russian entities with database breaches and data destruction, maintaining a low profile but believed to have connections to Ukrainian intelligence.

Handala Group, formed in December 2023, is an Iranian pro-Palestinian collective known for ransomware, data leaks, and psychological operations, targeting Israeli transportation, healthcare, technology, and government sectors. Their use of a professional website for publicity and data leaks distinguishes them within the hacktivist community.

Indian Cyber Force, initiated in December 2022, shows a pro-India and pro-Israel stance, conducting widespread attacks against nations like Pakistan, Indonesia, and Bangladesh. Their focus includes website defacements and sensitive data theft, often tied to historical and geopolitical grievances.

NoName057(16), a prolific Russian group dating back to March 2022, is heavily engaged in high-volume DDoS attacks targeting Ukraine and its allies, operating openly on social media while linked to Russian military cyber units through the Cyber Army of Russia Reborn.

Forescout’s report also notes the strategic advantages states gain by using hacktivism as a tool, such as plausible deniability, complicating attribution, creating the façade of popular support, and amplifying operational impacts through disinformation such as AI-generated imagery. This integration of cyberattacks with information warfare forms a core component of hybrid warfare strategies.

Looking ahead to 2025, Forescout predicts DDoS attacks will persist as a preferred method due to their ease of deployment by groups and supporters using accessible toolkits like DDoSia. The targeting of Internet of Things (IoT) and Operational Technology (OT) systems is expected to increase, driven by their potential for disruption. Critical infrastructure sectors that impact daily life, including government, financial services, and utilities, will remain key targets, with hacktivist actions adapting to the evolving geopolitical landscape of conflict zones such as Ukraine and Israel.

Security recommendations emphasised include adherence to guidance from the UK’s National Cyber Security Centre on denial-of-service attack mitigation, robust hardening of IoT and OT devices, network segmentation to prevent lateral movement during breaches, and enhanced monitoring for early detection of anomalous activity.

The Industrial Cyber publication is reporting that these findings underscore the rise in state-aligned hacktivism and its increasing impact on the global cyber threat environment. Concurrently, reports from Cyble indicate that hacktivists are expanding beyond traditional tactics, employing more destructive and sophisticated methods, including ransomware, particularly targeting critical infrastructure installations.

This comprehensive landscape reveals a complex, evolving interplay between hacktivism, state interests, and critical infrastructure security, shaping the future contours of cyber conflict and defence.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.forescout.com/press-releases/2024h1-threat-report/> - Forescout's 2024H1 Threat Review report highlights a 43% increase in published vulnerabilities compared to H1 2023, with 23,668 vulnerabilities reported in H1 2024, emphasizing the need for better device security.
* <https://industrialcyber.co/reports/forescout-2024-threat-report-warns-of-intensifying-cyber-threats-in-2025-as-ot-protocols-increasingly-targeted/> - The Industrial Cyber publication reports that Forescout's 2024 Threat Report warns of intensifying cyber threats in 2025, as OT protocols are increasingly targeted, underscoring the evolving nature of cyber conflicts tied to geopolitical tensions.
* <https://www.forescout.com/press-releases/2024h1-threat-report/> - Forescout's 2024H1 Threat Review report notes that state-sponsored actors are using hacktivist fronts to target critical infrastructure, with groups like Predatory Sparrow and Karma Power linked to significant attacks under the guise of hacktivism.
* <https://industrialcyber.co/reports/forescout-reports-cyber-threats-surge-state-sponsored-hackers-target-vpn-vulnerabilities-ransomware-attacks-rise/> - The Industrial Cyber publication reports that Forescout's 2024 Threat Report highlights a surge in cyber threats, with state-sponsored hackers targeting VPN vulnerabilities and a rise in ransomware attacks, indicating a shift in attack strategies.
* <https://www.forescout.com/press-releases/2024h1-threat-report/> - Forescout's 2024H1 Threat Review report reveals that the U.S., Germany, and India were the most targeted countries, with the U.S. being targeted twice as often as Germany and India, highlighting the global reach of cyber threats.
* <https://industrialcyber.co/reports/forescout-reports-cyber-threats-surge-state-sponsored-hackers-target-vpn-vulnerabilities-ransomware-attacks-rise/> - The Industrial Cyber publication reports that Forescout's 2024 Threat Report indicates a shift in attack strategies, with attackers moving from targeting managed endpoints to unmanaged perimeter devices due to their lack of visibility and security telemetry.
* <https://news.google.com/rss/articles/CBMizAFBVV95cUxNb2k1TG5uOUVSSG1obGJDbG5Jakxxbmh2aS05SjVpZWtBSWQ3T0RDNUtTWE5XRF9YbWhfdmtvcUtjX0FucFEzcmZ6eWdxYmdkN2dlN0J6ZGpSVU5xMW9aaXJuc3JGN1ozQjV2bEs0RWJDdnBfbmMxX2k4Q1lMc0RiRmtFNGJ5R1hseWFNUXQ2Z3RYODN6aVpjZ0ZuUTE3QzZWYmFnM2ZFTVpoUGwzTzR4dHVLampCOV81Z2Y4ckVnczBXcTR6ajFaXzlzaTA?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data