European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

June 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller

Overall observations

In **June 2024**, EuRepoC documented 60 cyber operations, representing a 17.8% decrease compared to the previous month. This total is eleven incidents below the overall average in recorded activity of 71 operations per month.

The **average intensity** of operations in June 2024 registered at 3.15, surpassing the historical average of 2.84. The elevated level of operations documented by the Repository since February 2023 is partly attributed to expanded inclusion criteria. As of March 2023, EuRepoC has systematically recorded operations conducted against critical infrastructure targets and no longer makes inclusion contingent on whether these activities are linked to political or governmental threat actors or victims.

About the briefing

The Cyber Conflict Briefing is an analytic product prepared by EuRepoC. The German edition is published in collaboration with the **Tagesspiegel Cybersecurity Background,** accessible here.
It summarises the key trends, dynamics, and findings on cyber incidents as recorded by EuRepoC in a given month. These do not necessarily have to have taken place in June, but may have started earlier. The focus is on technical, political, and legal aspects.

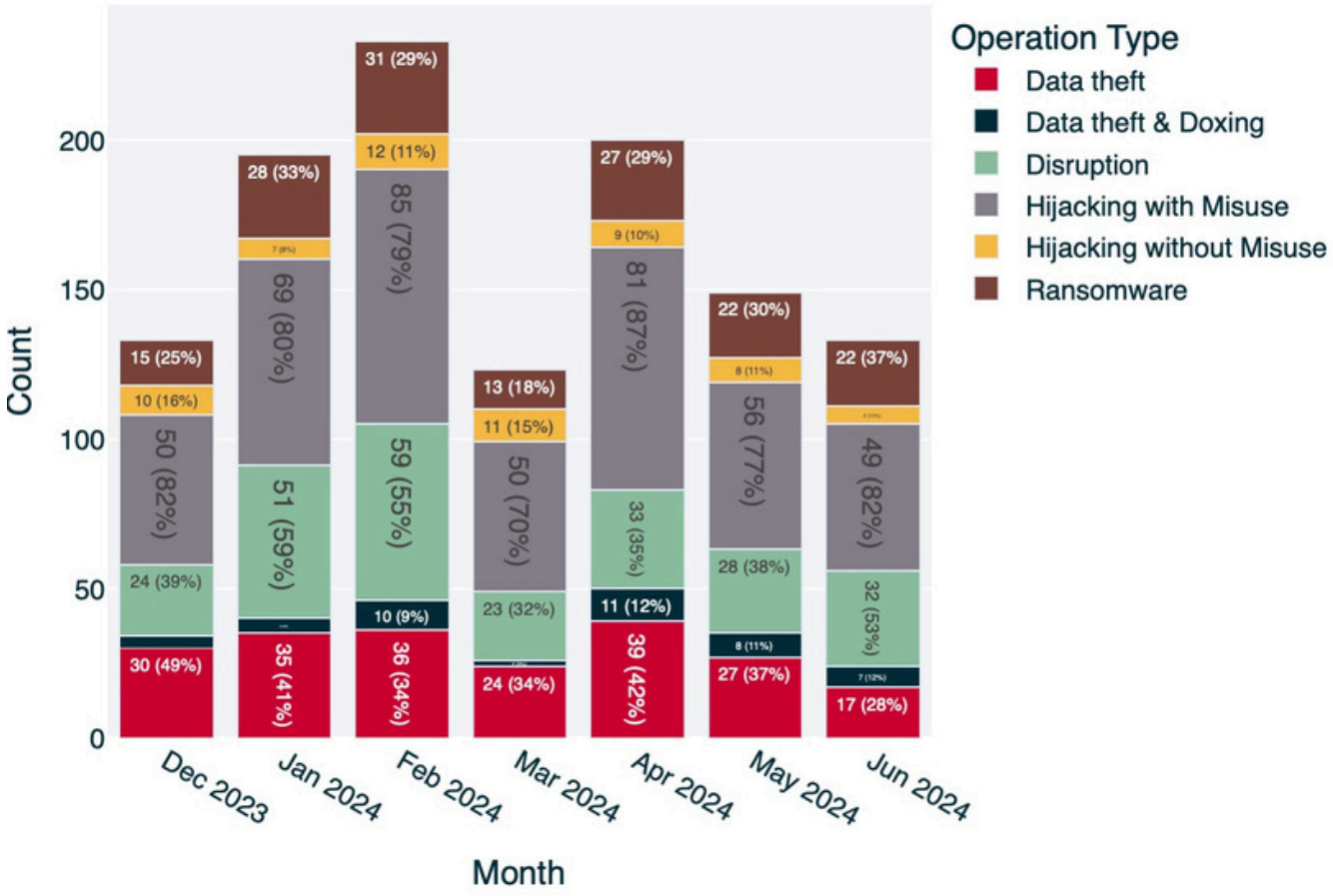
About EuRepoC

The European Repository of Cyber Incidents is a European research project with the aim of making information and knowledge about cyber conflicts visible. It is led by the University of Heidelberg, in cooperation with the University of Innsbruck, the Stiftung Wissenschaft und Politik and the Cyber Policy Institute (Estonia). It is currently funded by the German Federal Foreign Office and the Danish Ministry of Foreign Affairs.

Find out more at https://eurepoc.eu

The incidents recorded in June 2024 are distributed across the following **operation types**:

Monthly distribution of operations



Note: Individual cyber incidents may have several operation types in combination

The second most common type of operation identified in June 2024 was "disruption" operations (53%). These operations aim to disable IT services, impairing their availability. While disruption operations are typically temporary, ransomware can extend outages by blocking access to critical data for prolonged periods. EuRepoC recorded 32 such disruption operations in June.

The predominant activity observed in June, however, consisted of "hijacking with misuse" operations, with 49 cases comprising 82% of the total. This category encompasses operations where threat actors successfully infiltrate systems and networks to execute unauthorized and harmful actions. EuRepoC differentiates these activities based on the intent of the threat actors and identifies instances of data theft or operational disruption when applicable.

The motives behind activities may also overlap and evolve over time. Speculation to this effect arose in early June after the ransomware group BianLian published extensive data from the Australian mining company Northern Minerals. The leak included details of operational processes, project documents, research and development data, financial information, and

employee and investor data. On the same day, Australian Finance Minister Jim Chalmers had instructed five companies with links to China to sell their stakes in Northern Minerals, citing national interests. This timing has led to unconfirmed speculation in media reports that BianLian may have leaked internal information of the mining company in retaliation for this order, either at the direction of Chinese officials or on its own initiative to curry favour with the government.

Northern Minerals' mining activities in Australia include the development of strategically important reserves of rare earths. In the past, China's retaliation in response to investment and trade restrictions the government perceived unfair has repeatedly focussed on the state's control over the natural deposits and industrial processes used to extract these minerals. In July 2023, for instance, China's Ministry of Commerce responded to joint export controls on semiconductor manufacturing equipment by the US, Japan and the Netherlands by imposing export restrictions on rare earth elements, which are used in the production of computer chips. Later in 2023, the Chinese government extended an existing export ban to additional technologies used for processing rare earths.

Northern Minerals discovered BianLian's intrusion into its networks at the end of March. However, the company only publicly disclosed the incident on 4 June, the day after the stolen data was published.

It is not unusual for BianLian to hold off on leaking victim data. If targeted organisations engage in initial negotiations, the group may decide to publish stolen documents with some delay in cases where talks collapse.

Australia's Shadow Minister for Home Affairs, James Patterson, has called for a clear response from the government if it is found that BianLian's actions were state-sponsored.

Currently, there is no substantial evidence to suggest a combination of financial and geopolitical motives behind BianLian's actions. The temporal connection between the leak of Northern Minerals data and the sale of company shares ordered by the Australian government appears to be coincidental.

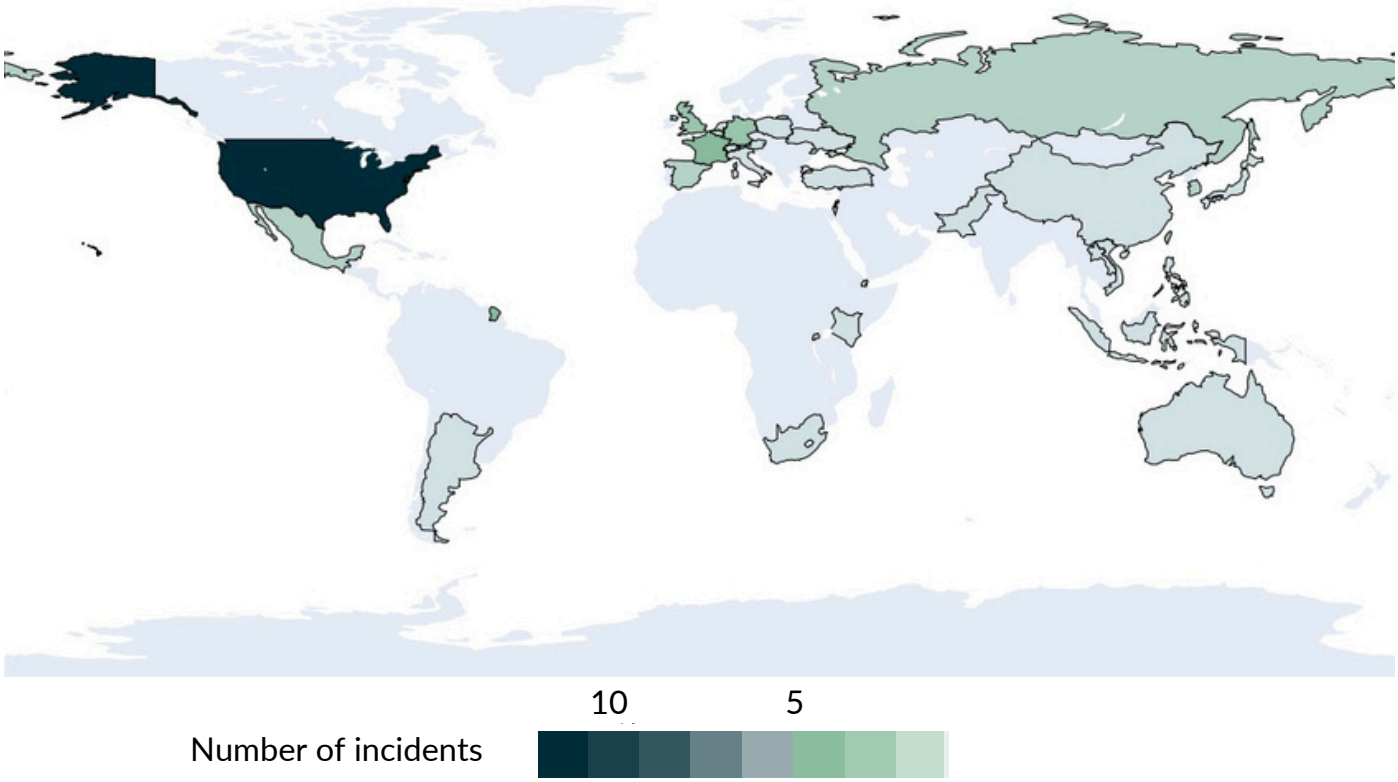
Focal points and targeting patterns

As in previous months, the most frequently targeted sector in June was critical infrastructure, with 36 cases or 60% of the recorded activity. Government institutions were the second most affected, with 25 cases (42%). In line with the overall declining trend in newly recorded incidents in June, the number of incidents affecting critical infrastructure fell by 20%. This drop is less pronounced for state institutions. For this target segment, case numbers fell by one incident compared to the previous month.

The United States remained the most affected country, with twelve incidents. Taken together, EU member states experienced a slightly higher number of incidents, totalling 16, with France and Germany being most frequently impacted, recording five and three incidents, respectively. Additionally, the Repository documented three incidents each for the UK and Taiwan.

The highest number of cases (eight) targeting critical infrastructure organisations were recorded for the financial sector.

Geographic distribution of operations



These were evenly split between service providers in the cryptocurrency sector and traditional financial companies. As in previous months, the cryptocurrency sector was almost exclusively affected by manipulations exploiting vulnerabilities in the protocols of these service providers for financial gain. In contrast, traditional financial companies were exclusively subjected to data theft. One such data breach in June affected a DZ Bank subsidiary in Germany. In these instances, threats to leak stolen data is frequently used as part of an extortion campaign against the compromised organisation, to pressure companies into negotiations with criminal groups, to avoid reputational damage or regulatory sanctions. Additionally, attackers may use the stolen data to facilitate further compromises, for example through targeted phishing campaigns that leverage hijacked email accounts to impersonate authentic contacts or modify internal documents to serve as phishing lures. The healthcare sector continued to be frequently affected, with seven cases in June.

In contrast to previous months, these incidents were not geographically concentrated in the US, but rather in Europe. For example, a ransomware attack against Synnovis, a service provider for the British National Health Service, made headlines, resulting in the postponement of important operations in the London area, among other things.

Among state institutions, sub-national governmental organizations were the most frequently targeted, with 16 incidents recorded in June. National-level institutions were affected to a considerably lesser degree, in five incidents. Specific targets were identified only in two cases, both in France. In mid-June, numerous French government websites were disrupted by DDoS attacks, rendering them temporarily unavailable. Additionally, ANSSI, the French cybersecurity agency, disclosed an espionage campaign against diplomatic organisations that has been ongoing since 2021. At a sub-national level, recorded threat activity did not exhibit a clear pattern.

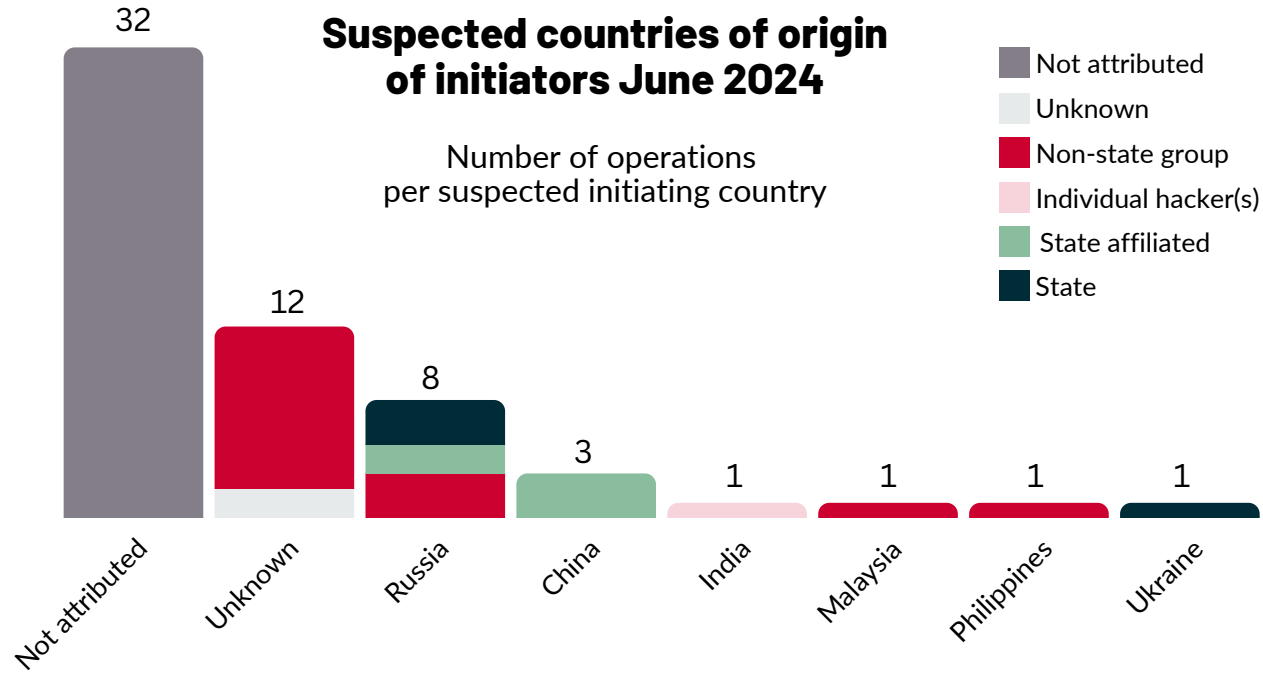
In addition to the consistently observed use of ransomware, politically-motivated incidents such as DDoS attacks or defacements were also recorded, for example for Belgium.

Threat actor profiles and attributions

At 53%, the proportion of unattributed incidents in June was 5% lower than in the previous month (58%). The proportion of operations that were linked to a specific type of attacker, but remained unattributed with respect to the country of origin, rose from 15% in May to 22% in June.

In a break from frequent observations, the incidents added to the Repository in June does not include activity originating from Iran or North Korea. Instead, recorded operations traced to Malaysia, the Philippines, and India, with one case each. In all three instances, non-state actors, with criminal, ideological, or personal motives were identified as the perpetrators. For example, the cybercrime group DragonForce targeted the public transport company O'ahu Transit Services in Hawai'i with ransomware. Doubt persists regarding attribution claims circulated in media reporting about Malaysia as the group's country of origin. A possible reason for this suspected link to Malaysia may be the conflation of the crime syndicate with the nearly identically named and better-known hacktivist group DragonForce Malaysia. While the group responsible for the O'ahu compromise focuses on financially motivated ransomware, DragonForce Malaysia is primarily involved in DDoS and defacement operations against Indian targets and has shown pro-Palestinian leanings in its actions against Israeli entities. DragonFroce Malaysia has denied any connection to the namesake ransomware group, a link purported by threat intelligence outlets. FalconFeeds, an Indian threat intelligence company, was among the first to report this distinction, reflecting that the victimology of both groups are potentially relevant for the geography of its clients. However, potential language and cultural barriers also constrain ransomware groups in their communications with victims, for example in the context of ransom negotiations. These challenges contribute to regional targeting patterns. Easily accessible generative AI tools and their integration into attack structures may gradually expand this regional focus. An exception to this modus operandi are Russian cybercrime gangs, which have entered into arrangements with authorities that exclude targets in their country of operation from their activities.

The case involving Indian perpetrators is also of interest, as it underscores the often underestimated threat posed by insiders. Threat models need to also account for former insiders in this regard, such as individuals that have recently left an organisation, especially if as a result of an unexpected lay-off. In one such instance, the Indian national Kandula Nagaraju accessed a test environment of the Singapore-based information technology company National Computer Systems (NCS) and deleted its 180 virtual servers during the period of January to March 2023. Nagaraju had been employed in the Quality Assurance (QA) department of NCS until his employment contract was terminated in October 2022. Following his termination, he began accessing the NCS network using his previous credentials, causing disruptions to company operations and $918,000 in damages.



A Singapore court subsequently found Nagaraju guilty of unauthorised access to computer material and sentenced him to two years and eight months in prison.

In June, the ongoing war between Russia and Ukraine once continued to dominate the threat activity observed in the context of conventional conflicts, with six incidents recorded for this dyad. Additionally, three other conflict dyads were documented, each with one associated operation: China-Taiwan; Israel-Hamas, et al.; and Vietnam, et al.-China in the context of the South China Sea disputes.

Russian intelligence services have previously drawn scrutiny for suspected dealings with cyber crime groups that are active in the post-Soviet space. At the core of these arrangements are assurances that law enforcement will "look the other way" when it comes to criminal activities, provided that Russian organisations are not being targeted and the hackers take on assignments as state proxies. An indictment of Amin Stigal, released by the US Department of Justice on 28 June, potentially shows that a collection of different motives pursued by criminal hackers with links to Russian intelligence attract the focus of authorities in target countries. The US indictment charges Stigal, who was born in the Chechen capital Grozny, with collaborated with Russia's military intelligence service GRU. Between August 2021 and February 2022, Stigal allegedly helped the GRU to break into Ukrainian networks, including to spread the WhisperGate wiper in the immediate run-up to Russia's military assault at the end of February 2022. Stigal and GRU conspirators reportedly not only targeted Ukrainian entities, but also US targets, both within the public and private sector. The indictment does not include further specifics on the cooperation between Stigal and the GRU or its origin. However, two aspects provide clues regarding Stigal's potential motivation. First, at age 22 Stigal is relatively young and reportedly started his career as hacker-for-hire at 19. This might make socialisation a factor. While limited to their respective jurisdictions, programmes such as the "Cyber Offender Prevention" initiative of the Dutch security authorities seek to provide options beyond criminal punishment to engage with technically skilful youth that had been involved in illegal activities, to offer alternative pathways.

Yet, especially in regions where young people have few opportunities on the labour market - which is the case for both Chechnya and the Republic of Dagestan, to which Stigal is also said to have links according to his FBI profile - the allure of quick gains through cybercrime is more challenging to overcome. Stigal's connection to Dagestan could also point to an ideological motive for the hacking operations in the Kremlin's service. Dagestan has been a stronghold for support of Putin in the recent past. A lack of economic prospects coupled with ideological conviction is a combination that makes non-state hackers particularly attractive to autocratic regimes and their security authorities. Both these enabling factors might apply to Stigal's case.

The activities of RedJuliett, or Flax Typhoon, underscore the PRC's strategic use of cyberspace to advance its geopolitical interests, particularly in regions like Asia and Africa. An espionage campaign, conducted by the group from November 2023 to April 2024, compromised 24 organizations across various sectors, including government, technology, science, and diplomacy. Although RedJuliett's operations mainly targeted Taiwan, its reach extended to entities in Hong Kong, Kenya, South Korea, Rwanda, Djibouti, Laos, and the United States.

While the espionage activities of RedJuliett reported by Recorded Future document notable tradecraft, they differ from those of another China-nexus group, Volt Typhoon. Last year, Volt Typhoon's infiltration of US critical infrastructure was classified by Microsoft not only as espionage but also as preparatory steps for potential acts of sabotage. No such assessments have been made for Flax Typhoon, suggesting a divergence in their operational objectives or tactics. In an upcoming APT profile covering the two groups, EuRepoC will provide a comparative analysis of Volt Typhoon and Flax Typhoon. This report will delve into the similarities and differences between these two groups, providing valuable insights into the evolving landscape of Chinese cyber operations

More from EuRepoC

EuRepoC informs about new entries in the Repository through a daily Cyber Incident Tracker, which is openly available for subscription.

About the authors

Jakob Bund is an Associate at the German Institute for International and Security Affairs (SWP).

Kerstin Zettl-Schabath is a Researcher at the Institute of Political Science (IPW) at Heidelberg University.

Martin Müller is a University Assistant and a doctoral candidate at the Institute for Theory and Future of Law at the University of Innsbruck.