European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

April 2023

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller
Camille Borrett (data support)

Overall observations

In **April 2023**, 63 cyber operations were recorded in the EuRepoC database. This is 28.41% less than the previous month, but still 15 operations (31.25%) more than the overall monthly average activity of 48 cyber operations.

The **average intensity** of operations recorded in April 2023 is 2.81, which is higher than the historical average (2.7). The striking increase in operations since February 2023 can also be explained primarily by the fact that, from March 2023 onwards, EuRepoC is recording all cyber attacks 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 April, but may have started earlier. The focus is on technical, political, and legal aspects.

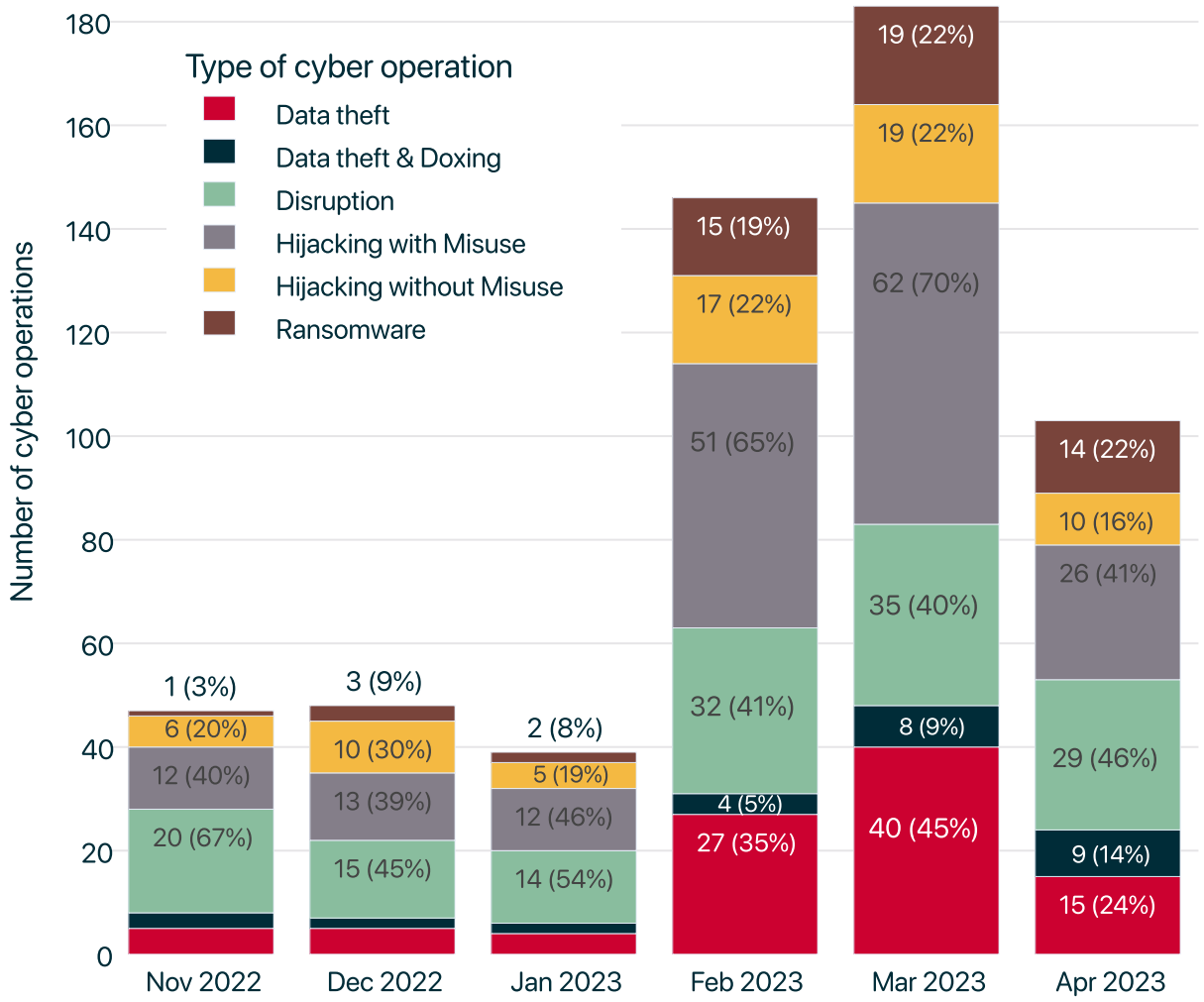
About EuRepoC

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 April 2023 are distributed across the following **operation types**:

Monthly distribution of operations



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

The largest share of incidents comprises **"disruption"** operations. These are operations with the aim of putting an information technology service out of operation. Accordingly, a disruption affects the availability of information. Disruption operations are generally temporary in nature, but they can also cause longer-term outages or, in extremely rare cases, permanent damage. Typical examples of disruption are DDoS attacks, which usually target publicly-accessible websites and, through a flood of access requests, bring the servers running the websites to their knees and make them temporarily inaccessible.

A more technically-sophisticated example of disruption operations is **ransomware attacks**, which encrypt data with extortionate intent and prevent work with digitally-stored information, directly impacting operations and possibly the business activities of affected organisations. Wiper tools, on the other hand, are designed to render devices permanently unusable and may be deployed for sabotage operations.

In the month of April, EuRepoC documented 29 of these disruption operations. DDoS attacks accounted for just under a third of these, which, if successfully carried out, are easily observable by all users regardless of technical analysis. Despite their generally negligible technical impact, these operations attract strong media attention because they are easily observable, which can increase the public's perception of the threat, reinforce the psychological effect, and thereby potentially abet the attackers' intentions.

In early April, reports of leaked U.S. intelligence documents pointed to activities of a pro-Russian hacktivist group that had infiltrated the networks of a Canadian gas pipeline company. According to the reports, the criminal group Zarya was allegedly able to increase valve pressure in sections of the pipeline and thus trigger emergency shutdowns.

Members of the group claimed the ability to do so to Russia's domestic intelligence service, the FSB. However, given the constant competition of hacktivist groups for the attention of state agencies, exaggerations of the group's actual means and capabilities cannot be ruled out. At a minimum, leaked U.S. intelligence reports speak of FSB officers subsequently monitoring Canadian intelligence more closely for signs of an explosion, anticipating that a successful operation would cause a detonation at a gas distribution station. Canadian Prime Minister Justin Trudeau appeared to confirm the incident during a press statement, acknowledging reports of the events while clarifying that there was no physical damage to Canadian energy infrastructure as a result of cyberattacks.

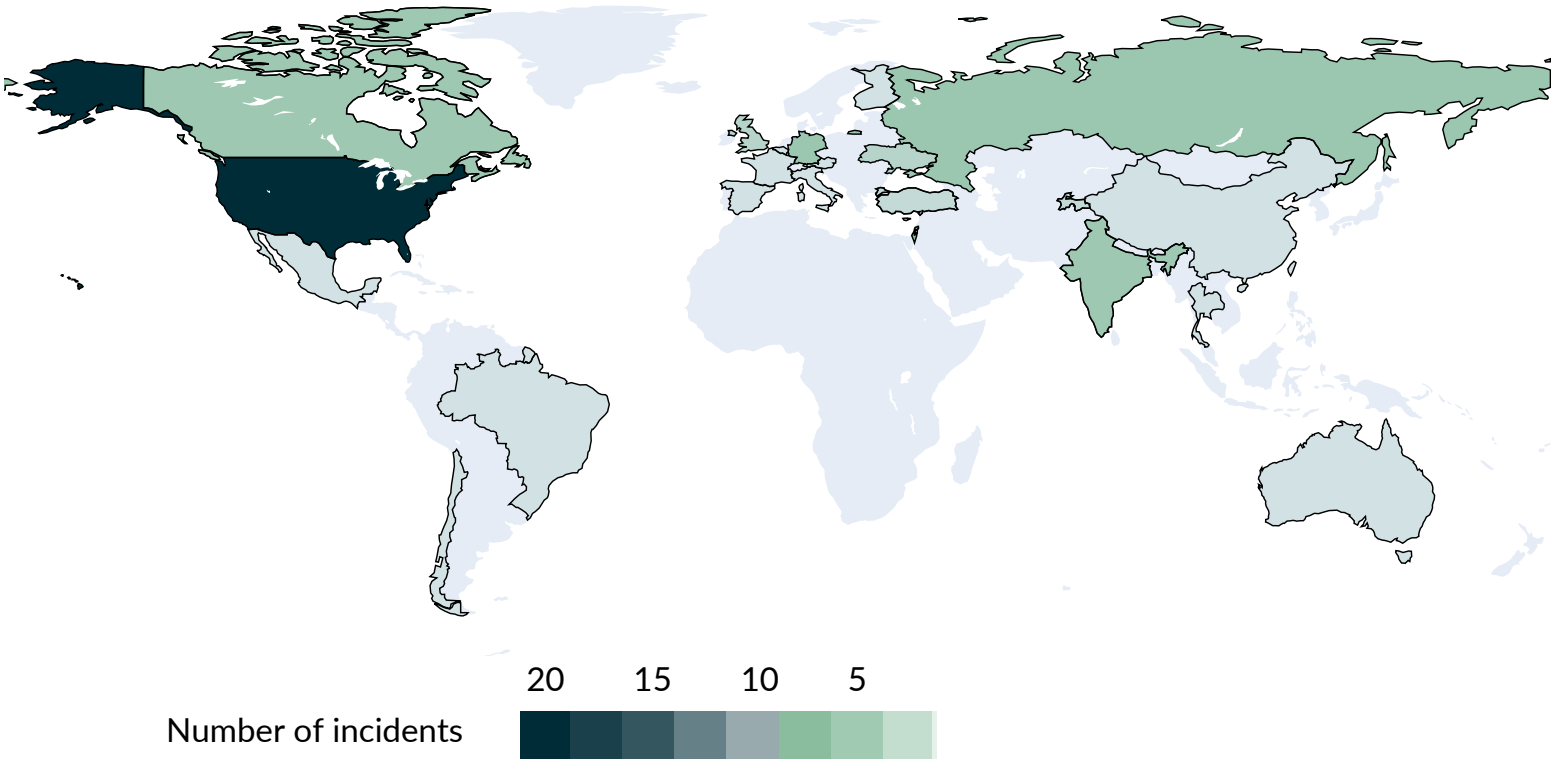
Further observation of the group's activities indicated that threat actors waited several days for further instructions, but were primarily interested in hurting the pipeline operator financially without damaging the infrastructure itself.

Doubts exist about Zarya's capabilities to effectively interfere with the operation of a pipeline. The grouping is a split-off of the Killnet collective, a group that has come to prominence primarily through DDoS attacks against international supporters of Ukraine. Disruptive actions against Western critical infrastructure, as in the case of the Canadian pipeline, have not yet been publicly attributed to non-state groups supporting Russia.

Shortly after these activities became known, the British government emphasised the danger posed by groups sympathetic to Russia. These ideologically-motivated actors operated opportunistically with the immediate goal of disrupting or destroying infrastructure. Unlike intelligence or military units, these non-state elements showed little restraint and, despite being guided by national interests, were outside state control.

The second most common type of operation recorded in April was "hijacking with misuse" operations. This strand describes actions in which attackers have managed to penetrate systems and networks to perform malicious, unauthorised actions. These activities, if identifiable, are further differentiated by intent and may include data theft or operational disruption. In April, EuRepoC recorded 26 such operations.

Geographic distribution of operations



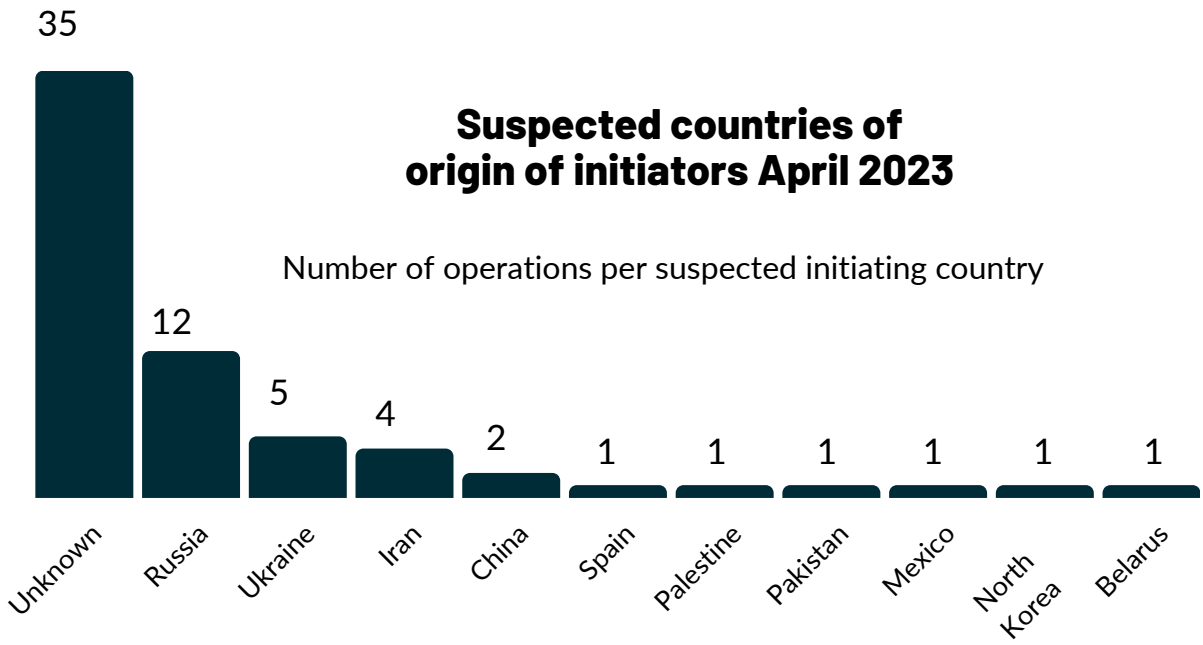
An example of this can be seen in the persistent espionage campaigns by the Winter Vivern group. As reported in last month's EuRepoC Cyber Conflict Briefing, its operations date back to 2021 and target victims on behalf of Russian and Belarusian interests. Winter Vivern's targeting patterns also reflect a heightened intelligence interest in U.S. and European deliberations and their assessments of the war dynamics in Ukraine. The sophisticated exploitation of a vulnerability in software from the manufacturer Zimbra in early 2023, which European governments use for their webmail portals, demonstrates Winter Vivern's characteristic efforts to tailor attack techniques to individual targets.

Also notable are attempts in which the group seeks to impersonate prominent experts and other knowledgeable individuals who have been in the limelight during the coverage of the war against Ukraine; these efforts seek to take advantage of the increased need for collaborative information sharing to develop access for the group's operations.

UK cybersecurity officials, among others, continue to point out in their situational awareness reports that espionage operations, such as Winter Vivern's, represent a major question mark in assessing what role cyber capabilities have played for Russia in waging war against Ukraine.

Focal points and targeting patterns

The affected countries recorded in April are predominantly distributed across Europe and North America, with almost two-thirds of the incidents taking place in these regions. The remaining one-third primarily involves cases in Israel (6 incidents), unspecified states in Africa (4), and India (2). Of the incidents in Europe and North America, the United States was the most affected (18), followed by Russia (5, counted as part of Europe), and Germany (4). The Russia-related incidents all took place in the context of the ongoing war against Ukraine.



The most frequently-targeted sector in April 2023 was critical infrastructure, with 50 cases and thus a share of almost 80% of all recorded cases. This stands in contrast to the previous month, in which government/political institutions or actors were most frequently targeted, with 67 cases. Here, a decrease of 66% to 22 cases took place. There are differences in the individual regions affected: in North America, for example, the most frequently-affected sector was healthcare, with incidents in hospitals occurring in several U.S. states and in Canada. This trend was also observed in Europe last month; therefore, a specific geographical reference cannot be identified, but rather a specific threat to the sector must be assumed.

In Europe, the focus in April was on the transportation and mechanical engineering sectors, with two incidents each, such as the Lürssen shipyard in Bremen. Other cases with a connection to Germany involved DDoS attacks by Russian "hacktivists" against the websites of police authorities in individual German states and the theft of e-mail credentials via the NATO School Oberammergau, presumably related to efforts to weaken support for Ukraine.

In many cases, the attribution of attacks has not been conclusively or publicly determined. In some cases, however, IT companies or governments have published indications of the possible regional origins of the operation (but not necessarily with respect to state responsibility).

Threat actor profiles and attributions

In April 2023, operations attributed to Russian actors continued to dominate on the attacker side. This was immediately followed by attackers with Ukrainian origins, which also indicates the continued high frequency of cyber incidents, but also persistently-elevated media presence of the war in general. After no incidents had been recorded for Iranian actors in March, there were four operations with attributed Iranian origin in April. Compared to the previous month (and also compared to other activity levels), the low number of operations with suspected Chinese origins (two incidents) is also striking. One reason for this may be that there were fewer incidents that met the EuRepoC inclusion criteria. Another reason could be that Chinese espionage operations, often designed to dwell undetected in compromised networks for sustained periods of time, are discovered with delay.

In addition to attributed operations, however, operations that could not (yet) be attributed to a specific country or actor again topped the list in April, accounting for 55.6% of cases (35).

In April, five operations stood out that were attributed to the group "Anonymous Sudan" or were directly claimed by this group. The exact background of the group is still disputed: while some observers from the threat intelligence industry now consider the group a Russian "false flag" operation, other circumstances speak for a possible integration of the (by its own account) Islamist-motivated grouping into the Russian hacktivist group Killnet, after Anonymous Sudan attacked pro-Ukrainian countries alongside attacks against Sweden and Denmark from mid-February (in response to a Qur'an burning). It seems to be clearer that the grouping has nothing to do with the original "Anonymous Sudan" group formed in 2019 in the wake of the military coup in Sudan. Four of the five operations added to the database in April were directed against Israeli targets, which could be taken as an indication of the group's purported pro-Islamist stance, despite public expressions of solidarity with Russia. On the other hand, cyber operations against Israel could also correspond to pro-Islamist/Palestinian as well as pro-Russian goals, following Israel's approval of the delivery of electronic drone interception systems to Ukraine in March. Ukraine-supporting states that have drawn the attention of the Islamist-leaning hacker community could thus continue to be an attractive target for Anonymous Sudan/Killnet to maintain the narrative intended obfuscate its identity.

The operation of the Iranian state-sponsored hacker group "Mango Sandstorm" (formerly "MERCURY," also known as "MuddyWater"), which was made public by Microsoft on 7 April, also exhibits patterns of concealing its identity. After Mango Sandstorm provided access to unspecified locally-installed software ("on-premises") and passed it on to the Iranian grouping Storm-1084 (formerly DEV-1084), the latter carried out disruptive operations (sometimes only after months of exploring the networks), which also targeted the cloud environment. This resulted in the destruction of a wide variety of resources, such as server farms, virtual machines, storage accounts, and virtual networks. According to Microsoft, Storm-1084 presents itself as an allegedly financially-motivated actor, presumably in order to hide its actual connection to Iranian state agencies, such as the Ministry of Intelligence and Security (MOIS), which has been linked to Mango Sandstorm by the U.S. Cyber Command.

April 2023 also saw 15 cyber incidents (6 more than in the previous month) attributed to the conventional conflict between Russia and Ukraine, which underlines the unabatedly-high level of activity of both pro-Ukrainian and pro-Russian hackers. For example, on 4 April, the pro-Russian group NoName057(16) attacked the websites of the Finnish Parliament and (former) Prime Minister Sanna Marin with DDoS operations, in the wake of the Nordic country's NATO accession.

In addition to these rather low-tech and mostly low-impact hacktivist operations, the Polish government announced on 13 April that the military counterintelligence service and the national Computer Emergency Response Team (CERT) had jointly uncovered an espionage operation by the Russian APT29 (aka Cozy Bear). This operation began back in October 2022 and targeted foreign ministries and diplomatic entities of NATO and EU countries (and, to a lesser extent, those in African countries). Notably, the Polish statement is transparent about the motivation for releasing the information, stating that the goal is "*to disrupt the ongoing espionage campaign, impose additional costs of operations against allied nations and enable the detection, analysis and tracking of the activity by affected parties and the wider cyber security industry*." Cyber espionage by high-profile Russian APTs thus remains an important tool for the Kremlin to shape its own war strategy as well as to inform higher-level policy decisions.

The fact that the telecommunications sector in African countries in particular was repeatedly targeted by foreign cyber espionage (seven incidents in the dataset) was further demonstrated by a report from the threat intelligence firm Symantec from 20 April, which described an espionage operation by the Chinese-language APT "Daggerfly" (aka "Evasive Panda") beginning in November 2022. In the same report, Symantec also made public the apparent continuation of the "Tainted Love" spying operation, which was disclosed by SentinelOne in March. Based on these findings, the APT "Othorene" (aka "Gallium"), also suspected to be Chinese, was held responsible for operations against telecommunications companies in Africa and the Middle East (according to assessments with "moderate confidence"), which also began in November 2022.

The lower level of certainty attached to this attribution statement reflects the high level of "TTP-sharing/diffusion" by Chinese groups (TTP = Tactics, Techniques, and Procedures), which makes it difficult to assign responsibility to individual groups. Telecommunications companies not only represent an attractive primary target for espionage (especially due to commercial interest in this sector in African economies), but can also function as a helpful gateway to obtain information (e.g., via supply chain operations) from targeted customers.

More from EuRepoC

From 11-12 May, EuRepoC hosted an interdisciplinary workshop titled "*New Threats, New Methods, New Norms: Current Developments in Cybersecurity Theory and Law*" in Innsbruck, with external participants from politics, academia, and the threat intelligence industry taking part. Drawing on insights from EuRepoC data, workshop discussions focused on current attacker trends (in Ukraine and beyond), the status of a potential European attribution process, and lessons for systematically assessing the international law and technical dimension of cyber operations.

On 25 May, EuRepoC published an APT profile on the Russian/Belarusian group UNC1151, which is deemed responsible for the Ghostwriter campaign and stands out for its combination of hacking and disinformation tactics.

EuRepoC provides information on new cyber incidents added to its database through a daily curated Cyber Incident Tracker. You can subscribe to this here.

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.

Camille Borrett is a Data Analyst at the German Institute for International and Security Affairs (SWP).

Follow us on social media


@EuRepoC


linkedin/EuRepoC


contact@eurepoc.eu


https://eurepoc.eu