European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

April 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller
Camille Borrett (Data Support)

Overall observations

In **April 2024**, EuRepoC documented 94 cyber operations, representing a 32.4% increase compared to the previous month. This figure is 22 incidents higher than the overall average in recorded activity of 72 cyber operations per month.

The **average intensity** of operations in April 2024 registered at 3.42, surpassing the historical average of 2.82. 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 April, but may have started earlier. The focus is on technical, political, and legal aspects.

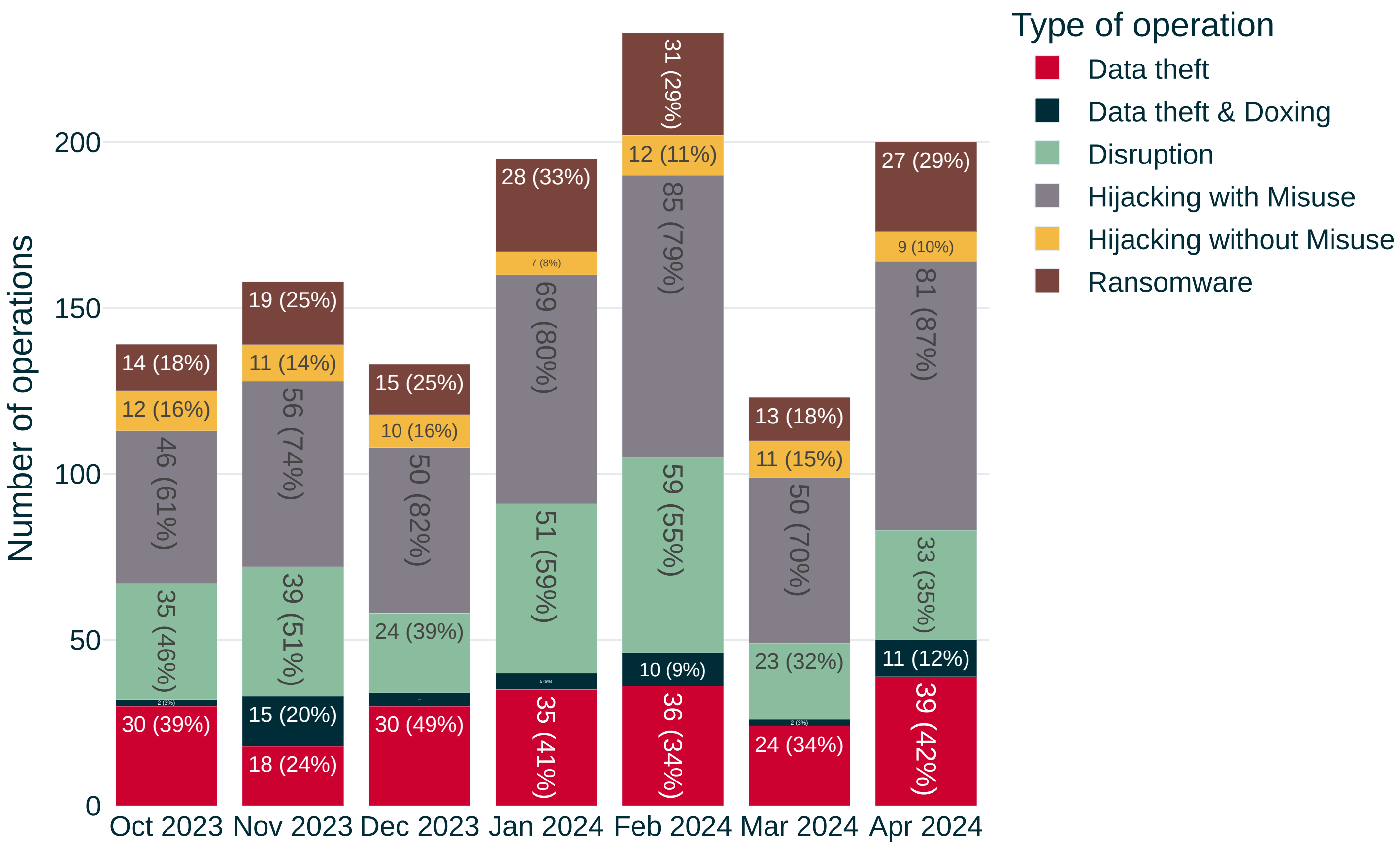
About EuRepoC

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 2024 are distributed across the following **operation types**:

Monthly distribution of operations



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

In April, the predominant activity observed consisted of **"hijacking with misuse"** operations, comprising 81 cases and accounting for 87% of the total. The second most frequently observed activity was “data theft” operations, covering 42% of the incidents. The Repository recorded 39 such incidents this month.

As observed in the previous Briefing, the theft and deletion of data critical to business continuity serve not only as a pressure tactic for financially motivated criminal actors but also as tools for hacktivist groups to achieve political goals. In April, the Cyber Partisans, a hacktivist group formed in 2020 to oppose repressive actions of the Lukashenko regime in Belarus, employed this tactic. The group encrypted several hundred work computers and deleted databases, backups, and email archives from Hrodna Azot, a major chemical company and one of the country's largest enterprises. Additionally, the collective gained access to the company’s surveillance systems.

Members of the Cyber Partisans had previously spent several months conducting reconnaissance on the company's networks. By its own account, the group gained extensive access to control systems, allegedly enabling it to halt production at the plant altogether.

To prevent collateral damage to employees and avoid long-lasting effects for the population as a result of disruptions to production, members of the group switched off the heating system instead - a system that it knew could be substituted for by backup sources.

In return for restored access to the blocked systems, the Cyber Partisans demanded the release of company employees and 75 other political prisoners in precarious medical conditions. Following protests against the official election results, which awarded Lukashenko a sixth term as president in 2020, workers at the plant were repeatedly detained, intimidated, and dismissed by the company's management under what appeared to be politically motivated pretexts. Against this backdrop, the US and the EU imposed sanctions on Hrodna Azot in 2021, with Japan and Ukraine joining in 2022.

Referring to these measures, the Cyber Partisans styled their actions against Hrodna Azot as "cyber sanctions." The group indicated that other companies and organisations involved in political repression in Belarus are part of its targeting strategy.

In its account of the incident, the group emphasised that it was not utilising all of its capabilities. The group warned of further actions against the company, should its demands remained unmet.

To underscore this message and stress its commitment to its demands, on 3 May, the Cyber Partisans initiated the time-controlled deletion of additional data from servers within networks that Hrodna Azot had supposedly secured.

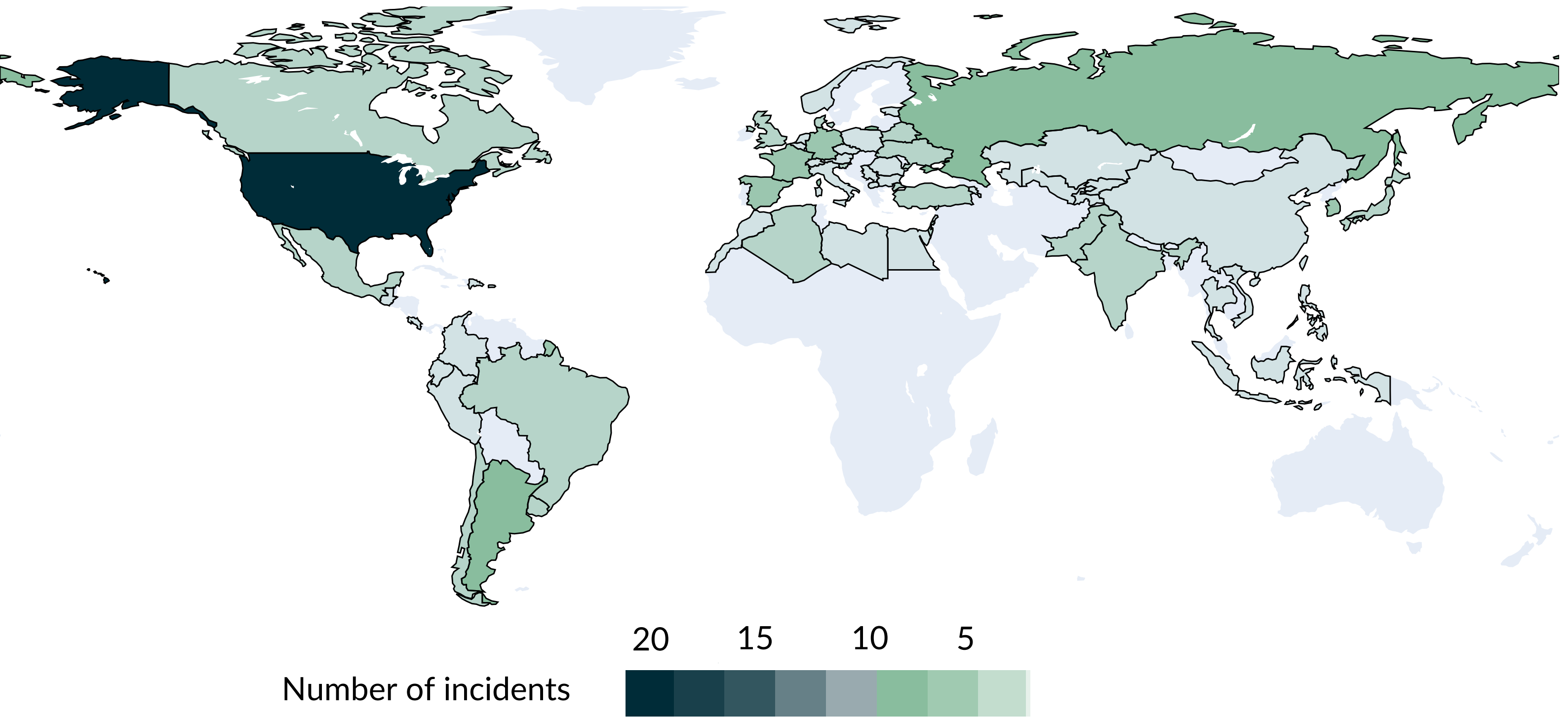
Focal points and targeting patterns

In April, critical infrastructure was the most frequently targeted sector, with 54 incidents, corresponding to 57% of the newly recorded cases. State institutions were the second most targeted, with 42 cases (45%). Following the significant decline in cases in March, this represents an increase compared to February for both critical infrastructure (up 64%) and state institutions (up 17%).

The United States was again the most affected country in April, with 24 incidents. Member states of the European Union were similarly affected, with 23 cases recorded for the bloc. Compared to March, the figures remained at almost the same level. In contrast, the number of incidents affecting targets outside the EU and the US increased. For example, Russia and Argentina each experienced seven incidents. At the country level, Germany and Spain follow these statistics as the most frequently affected EU member states, with six incidents each.

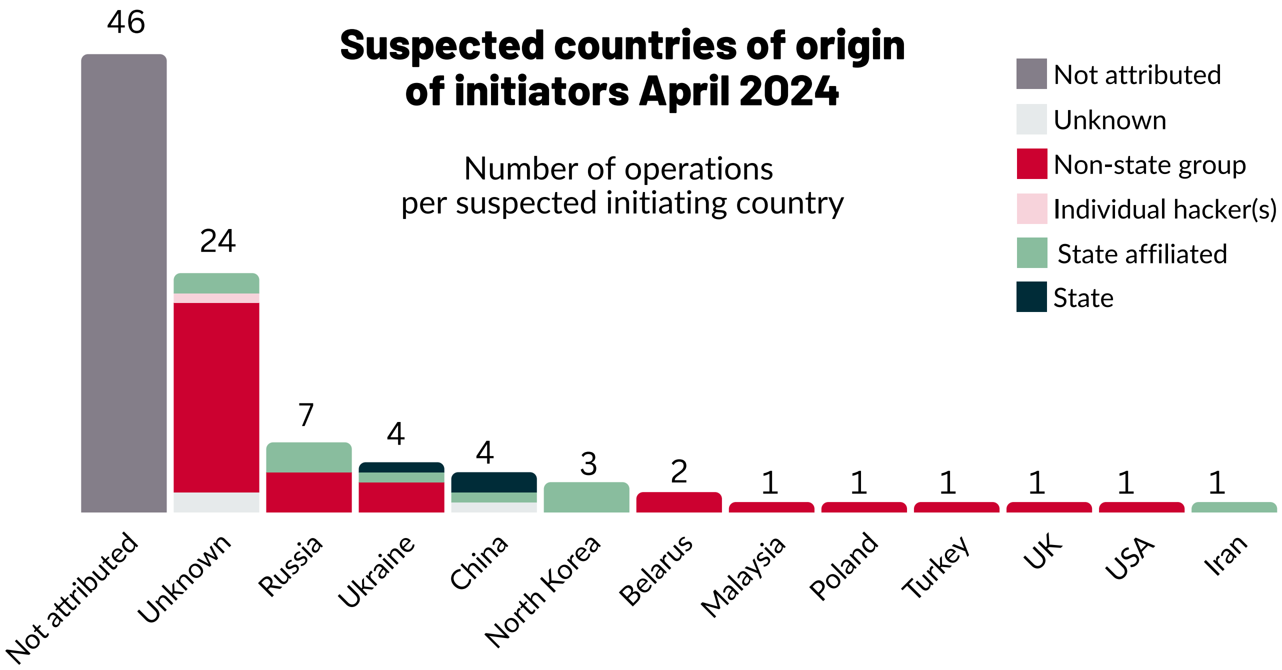
Among critical infrastructure targets, almost a third (17 incidents) were in the healthcare sector, with half of these incidents occurring in the United States. The sensitivity of healthcare data makes this sector a particularly sought-after target space for data theft, which was observed in eleven incidents in April. Although attribution is pending in many cases, identified perpetrators are almost exclusively ransomware groups.

Geographic distribution of operations



The second most affected sector was critical manufacturing, with eight incidents. Criminal groups were also actively targeting this sector. Given the salience of proprietary processes and technologies, the sector remains in the focus of industrial espionage campaigns. One such case involving the theft of confidential information from the Volkswagen Group in Germany, publicly disclosed in April, and was attributed to Chinese state actors. Digital service providers and the financial sector were also frequently affected, with six incidents. For these operations targeting service providers, ransomware groups were involved in incidents in Switzerland and Chile. In a separate case, state actors exploited a zero-day vulnerability at the IT security company Palo Alto Networks. The financial sector, which has seen frequent entries in the database in recent months in connection with thefts from crypto platforms, also experienced disruptive attacks.

Among state institutions, regional and local authorities remain a frequent focus. In April, around two-thirds of incidents targeting state institutions involved authorities at the subnational level. This observation supports the assumption that local institutions, which typically operate with fewer resources, face trade-offs in their security investments that may leave them vulnerable to opportunistic criminal actors. This assumption about the role of criminal actors remains under scrutiny, as the perpetrators have not been publicly identified in almost two-thirds of these incidents. A similar attribution pattern emerged for national organisations. Smaller countries in particular, including the Dominican Republic and Palau, reported data theft from governmental ministries. In addition, two incidents of data theft were recorded at the Israeli Ministry of Defence and the Ministry of Justice. These incidents exhibited hallmarks of hacktivism and are suspected to be linked to Israel's military operations in the Gaza Strip.



Threat actor profiles and attributions

The proportion of completely unattributed cyber incidents was slightly lower in April, at 49%, compared to 54% in March. The share of operations for which the type of attacker had been identified, but not the country of origin, remained almost identical, at 24% (March: 25%). In contrast, the list of countries of origin of the incidents added to the Repository in April more than doubled compared to February. While only Russia, China, North Korea, Iran, and Ukraine were recorded as points of origin in March, the list for April comprises eleven different countries, including the US, the UK, and Poland. A single incident significantly contributed to this increase. At the beginning of April, the pro-Ukrainian hacker group OneFist was revealed to have stolen 100 GB of data from the Russian defence company Special Technological Center LLC (STC) earlier in January. Although the Ukrainian Ministry of Defence had already reported in January that STC data had been leaked to them, the Ministry at the time did not disclose the source or method through which the data was acquired. Prior to OneFist's confirmation of the compromise, this left open the possibility that the breach could have been an inside job. For this reason, the incident was only added to the Repository in April. The case of OneFist, with members reportedly based in the US, the UK, and Poland (as well as five other unspecified countries), furthermore underscores the political and international law issues surrounding non-state hackers' involvement in the Russian-Ukrainian conflict. Since the outbreak of hostilities in February 2022, the government of Ukraine has not only helped establish independent hacktivist outfits, such as the IT Army of Ukraine, but has presumably also played an instrumental role in steering their activities. Recently, Ukraine awarded OneFist recognition for its operations against Russia. Members, including the American Kristopher Kortright (alias "Voltage"), received certificates for "significant contributions to the development and maintenance of vital military activities." This recognition not only highlights contributions of local civilians but also foreign citizens in a military context, potentially making them legitimate targets of military reprisals by Russia under international law. Furthermore, such hacktivist operations carry the risk of unintended consequences or spill-over effects, including for Ukraine or its international supporters.

In a post-war scenario, there is also the question of what individuals currently involved in hacktivist campaigning will shift to, once the motivation to turn their resources against Russian targets wears off. Cases like Kortright's are also worth tracking to understand the personal cost incurred by hacktivists that may become a factor in these post-war developments. Kortright claims to have lost his job because of his hacking activities.

Two other noteworthy attributions in April concerned Belarusian actors. Both cases involved hacktivist operations by the Cyber Partisans, a group composed of Belarusian IT professionals living abroad, according to reporting by the Washington Post. In addition to the aforementioned case against the Hrodna Azot chemical plant, the group claimed at the end of April to have compromised the networks of the Belarusian secret service KGB in autumn 2023, obtaining the personnel files of over 8,000 current and former employees. Although the group had demonstrated a pro-Ukrainian stance before Russia's February 2022 invasion through hacking operations against the Belarusian rail network used by Moscow to mass its forces at the borders of Ukraine, its operations are essentially directed against Lukashenko. Internal information obtained from regime institutions during earlier compromises could develop additional relevance in the future, for example should Lukashenko or other high-ranking officials be indicted by the International Criminal Court over Belarusian activity in Ukraine. Autocratic regimes are already attempting to thwart such potential cases through cyber operations, as illustrated by reported Russian efforts to delete or steal evidence of possible war crimes under investigation in Ukraine.

In April, 17 cyber operations were attributed to conventional conflicts. Connections to seven different conflict dyads show a significantly larger spread of activity compared to earlier months. Previously, the war of Russia against Ukraine and, since October 2023, the Israel-Hamas dyad had dominated. In April, however, operations were recorded in the context of other, often long-standing if not always armed conflicts. These constellations included Belarus vs. opposition; EU, US, et al. vs. Russia; North Korea vs. South Korea; Iran vs. Israel; and China vs. US. Numerically, Russia's war against Ukraine continued to dominate cyber conflict activity in April, with seven recorded incidents, followed by three operations related to the inter-Korean conflict and three linked to the Israel-Hamas dyad.

More from EuRepoC

EuRepoC informs about new cyber incidents added to the database with a Cyber Incident Tracker, updated daily. You can subscribe 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