European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

May 2023

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

Overall observations

In May 2023, the **EuRepoC database** recorded 112 cyber operations. This marks an increase of more than 77.8% compared to the previous month. At this level, activity recorded in May exceeded the overall average of 60 cyber operations per month by 52 operations.

The **average intensity** of operations recorded in May 2023 stood at 3.13, above the historical average of 2.5. The striking increase in operations since February 2023 is partly explained 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. These changes in scope notwithstanding, the number of recorded cyber operations in May are significantly higher than observations for March and April.

About the briefing

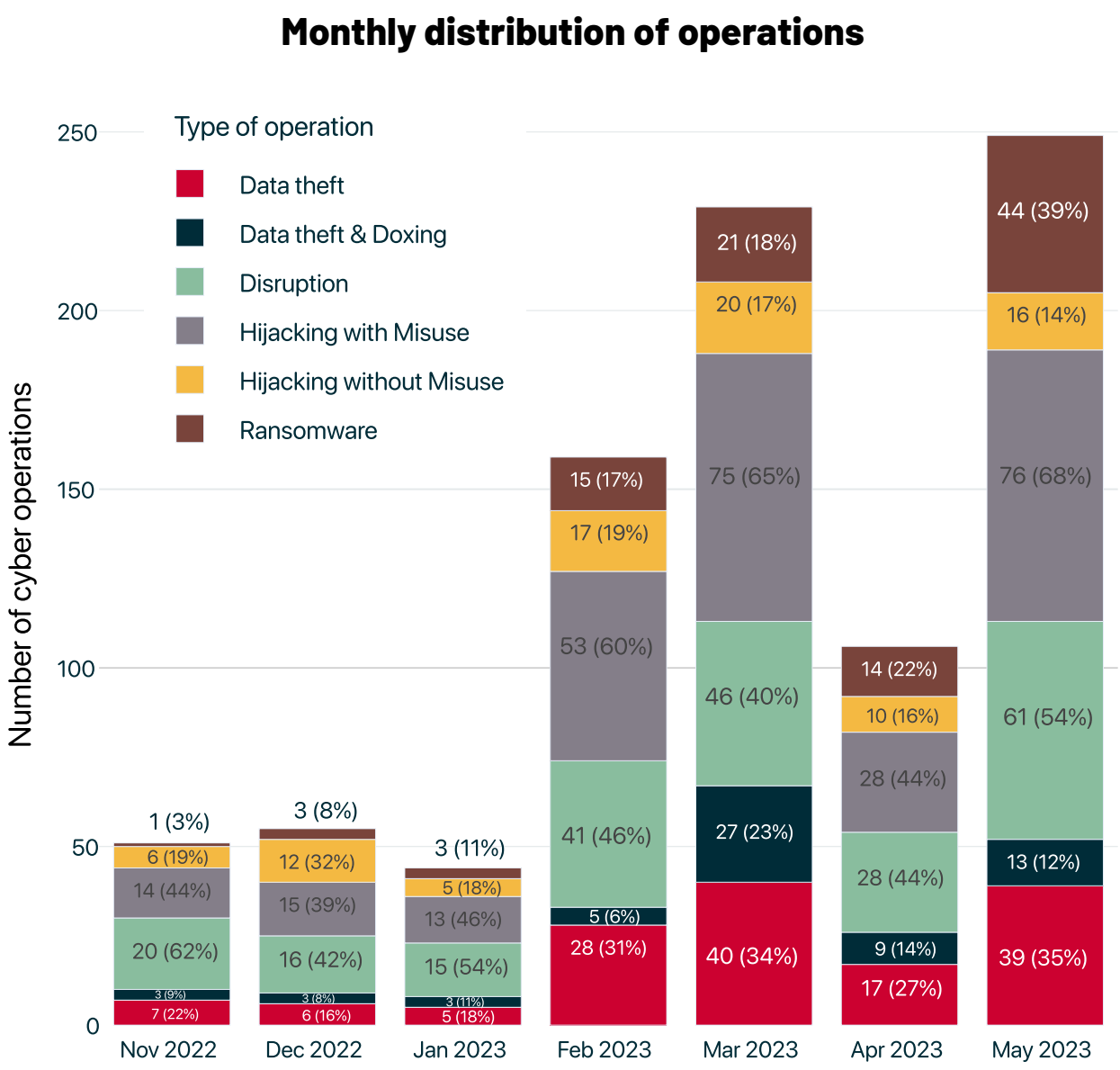
The Cyber Conflict Briefing is an analytic product prepared by EuRepoC. The German edition is published in collaboration with the **Tagesspiegel Cybersecurity Background,** accessible here.
It summarises the key trends, dynamics, and findings on cyber incidents as recorded by EuRepoC in a given month. These do not necessarily have to have taken place in May, 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 May 2023 are distributed across the following **operation types**:



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

The largest share of activity comprises "**hijacking with misuse**" operations (76%). As a an umbrella term, this describes operations in which threat actors have succeeded in penetrating systems and networks to carry out unauthorised, harmful actions. Where collection on these indicators is possible, EuRepoC differentiates these activities further by attacker intent and, if applicable, tracks data theft or operational disruptions.

Notable among these operation were actions of Volt Typhoon (also known as BRONZE SILHOUETTE/Vanguard Panda), a group with suspeced ties to the Chinese government, disclosed by Microsoft and the Five Eyes intelligence alliance on the same day (24 May).

This espionage campaign has been targeting critical infrastructure in the United States. The Five Eye authorities responsible for the report expect that techniques similar to those used in the campaign could be deployed worldwide. In an independent assessment, Microsoft came to the conclusion that the observed operations are aimed at gathering intelligence in order to cut off important communication channels between the US and Asia in the event of a future crisis.

The Volt Typhoon campaign is characterised by the use of so-called "living-off-the-land" tactics. Borrowing from the example of Napoleonic troops exploiting conquered territory, this approach aims to make an attacker's own advance independent of supply lines. In the context of cyber operations, instead of looting granaries, threat actors rely on the clever use of the targets' own network management tools. These tactics are primarily used to make attacks blend inconspicuously into typical data traffic and normal usage behaviour, to avoid detection.

Even after signs of compromise are known and documented, this approach can pose further challenges to the detection of a threat actor. Distinguishing between legitimate and malicious behaviour requires intimate knowledge of common network movements, which puts the onus to classify any false positives on potential targets.

In a new development, the credit rating agency Moody's reflected the reporting in a credit negative assessment for entities in the US communications, energy, and transportation sectors. For the first time citing the risks presented in a regulatory cybersecurity advisory, Moody's linked this finding to the expected reduction in revenue and liquidity in the case of a disruption, but also longer-term reputational damage, litigation, or - and remarkably independent of the actual occurrence of such an incident - risks of increased regulatory oversight.

"**Disruption**" operations accounted for the second-most common type of operation recorded in May. These are operations aimed at putting an information technology service out of operation. A disruption operation thus affects its availability. Disruption operations are generally temporary in effect. This transitory nature is partly rooted in the concern of attackers to manage escalation risks by ensuring effects are reversible and partly a result of the tools most commonly deployed. The majority of operations remain DDoS attacks that overwhelm websites only for the limited duration of their avalanche of access requests. Also frequently-recorded were so-called "defacement" attacks, in which websites are not only paralysed, but also papered over ("defaced") with mostly politically or ideologically-motivated content. Technically more-sophisticated operations, such as ransomware attacks that encrypt business-critical data or targeted sabotage actions, can also cause longer-term outages or, in extremely rare cases, permanent (even physical) damage. Of these actions committed with disruptive intent, EuRepoC recorded a total of 61 for May. None of these incidents caused physical effects or damage, indicating the prevalence of less intensive DDoS/defacement operations and ransomware attacks.

In distinction from actions aimed at causing damage, disruptive actions are also conducted for cybersecurity purposes. The FBI's dismantling of attack infrastructure belonging to the Russian espionage group Turla in early May is an example of such operational intervention to prevent attacks.

Turla is attributed by the US government to a unit of the Russian domestic intelligence service FSB and is considered one of the oldest continuously-active cyber actors. For more than 20 years, the group maintained a espionage network linked worldwide by the Snake malware, which is hidden deep within infected systems and networks. The malware was active on several hundred computers in more than 50 countries. Turla regularly evolved Snake capabilities and updated it on target systems controlled by the group to avoid discovery.

In the past, Turla has succeeded in staying undetected for long periods and exfiltrating information obtained from a number of targeted networks. In Germany, for example, the German Foreign Office announced a cyberattack in 2018, which media reports linked to Snake.

After joint monitoring with allies and private-sector partners, the FBI obtained a search warrant on 8 May that allowed investigators to run a specially-developed program on infected systems in the United States. The FBI's software caused Snake to overwrite and neutralise itself.

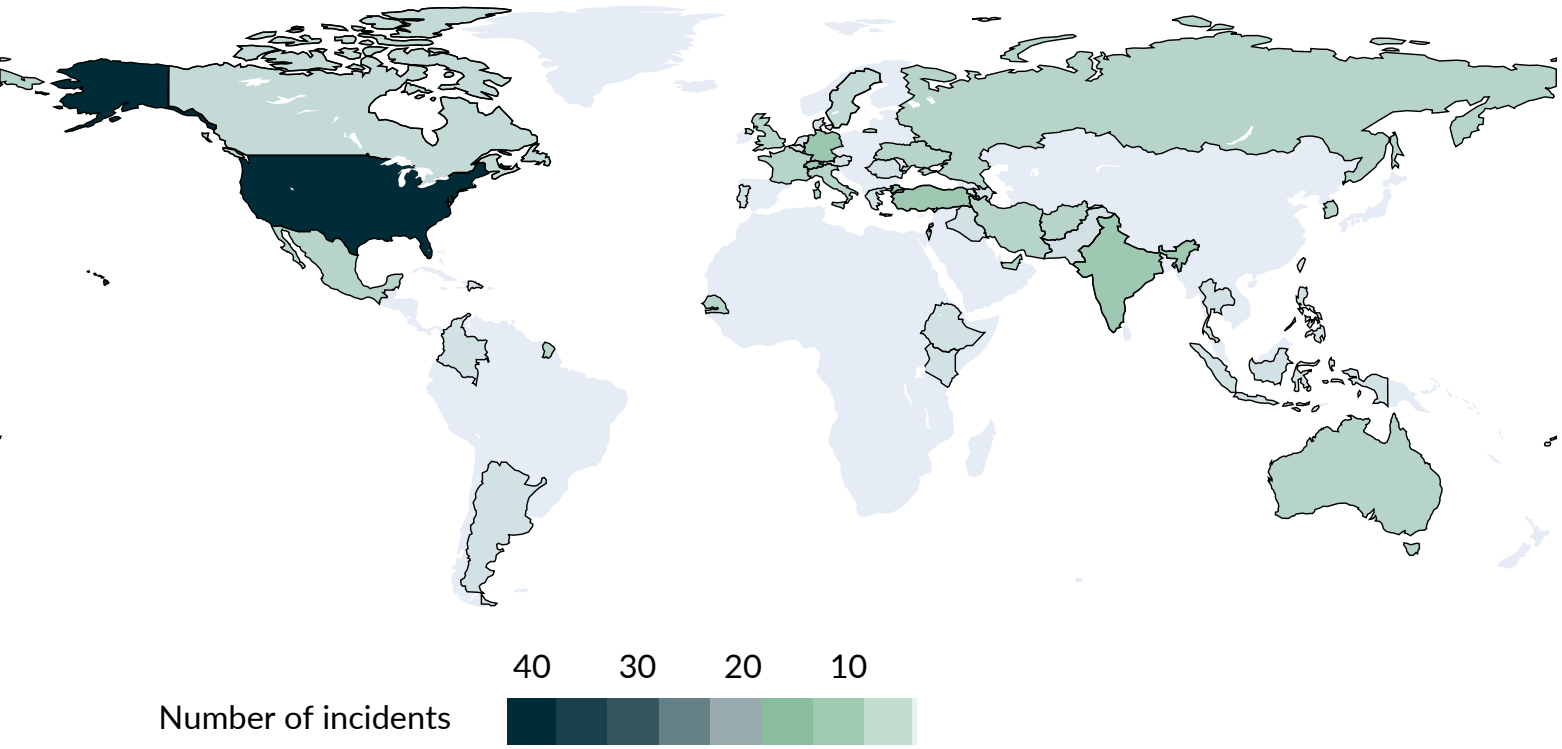
This approach points to further expansions in the use cases of investigation and law enforcement methods, which no longer focus solely on prosecuting responsible perpetrators, but increasingly also on weakening the attack capabilities of threat actors to prevent malicious activity or at least reduce its potential for damage.

Focal points and targeting patterns

A look at the distribution of cyber incidents among the targeted states shows - as in previous months - that the United States was by far the most affected. In May, cases concerning the US accounted for almost a third of all recorded operations (40), which roughly matches the proportion of previous months. Germany was the second-most affected country, with six incidents, making it the most frequently-targeted EU member state, also as in the previous month. Overall, EU member states were among reported targets in about one-fifth of all incidents (25). The distribution reflects the US's significantly larger attack surface and the globally prominent position of its industrial and technological sectors, as commercially successful and systemically relevant companies and institutions may additonally raise a country's profile as target for cyber espionage and ransomware operations. Lastly, the salient (geo)political position of the US may further expose it to politically-motivated attacks in addition to the commercial motives of cybercrime groups.

In May 2023, critical infrastructure targets were affected in just under half of the recorded cases, tallying up to 56 cases; from an absolute perspective, this is in line with the number of cases recorded in the previous month (50). Following closely behind are government institutions as affected sectors, accounting for 54 cases, or 48% of the total, marking a noticeable increase compared to the 22 cases of the previous month.

Geographic distribution of operations



Among the cases in which EU member states were affected, the most frequent attacks against critical infrastructure targets homed in on the subsector of “critical manufacturing,” with five recorded cases in May. In Germany, this affected the defence company Rheinmetall and the automotive spare parts dealer Bilstein Group. Both cases have been attributed to known ransomware groups.

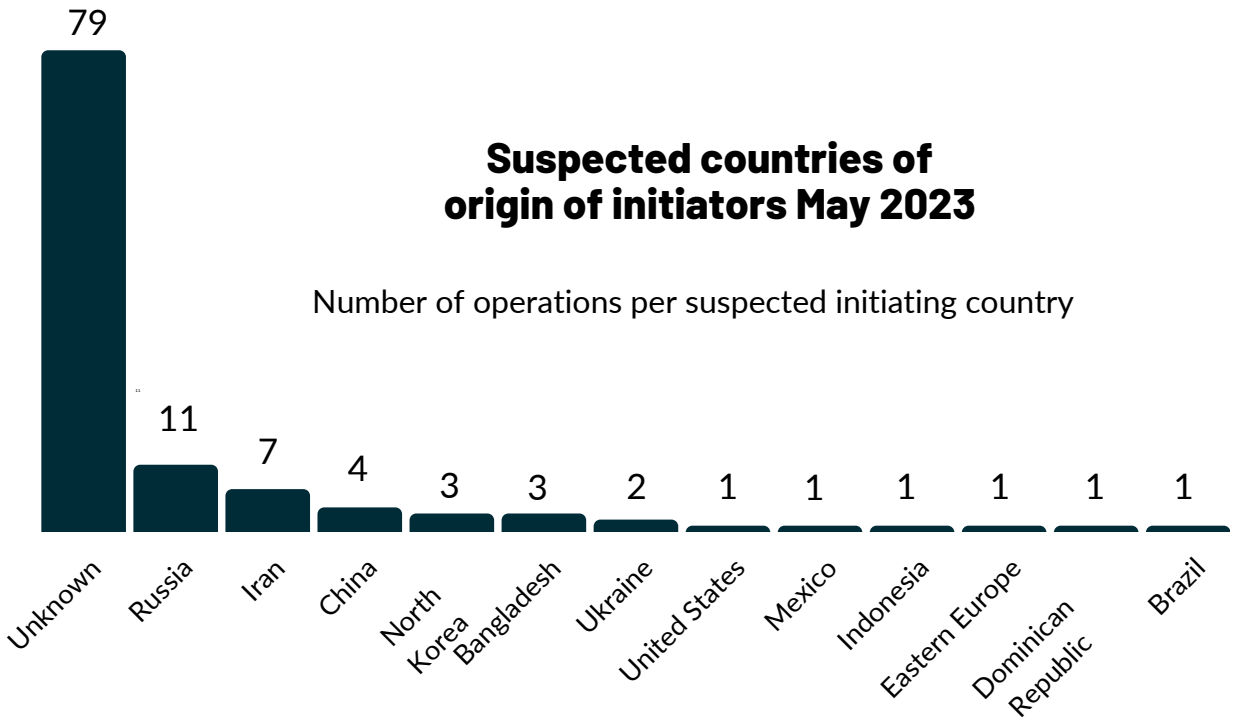
Cases with targets in the public administration largely involved educational institutions or associated administrative authorities (14 incidents), such as the Department of Education of the City of Basel in Switzerland.

Following in this pattern, regional and local authorities are disproportionately affected, possibly reflecting lower levels of protection compared to authorities at the national level.

Threat actors often remain unknown or unreported, potentially indicating a more opportunistic rather than target-specific approach, sometimes supported by the use of ransomware.

Threat actor profiles and attributions

The trend of the past months that the majority of recorded operations have not yet been attributed to a country of origin continued through May (79 out of 112 cases). Among attributed cases, threat actors of suspected Russian origin were most frequently identified as responsible for cyber operations in May, totaling 11 cases - one less than in the previous month.



The increase in cases attributed to Iran noted in April consolidated in May, with 7 associated cases. Operations attributed to Ukrainian actors fell slightly in May compared to the previous month (5), with only two incidents. All four operations attributed to Chinese actors are classified as "advanced persistent threats" (APTs) - an identifier commonly used for groups directed or supported by states.

As observed in the past for Chinese groups, cases centred on cyber-enabled espionage lined to reported data theft or the dormant infiltration of target systems to faciliate the exfiltration of data at a later stage or to preposition capabilities for sabotage operations in the event of escalating conflicts. This latter concern was expressed by Microsoft in its aforementioned report about the operations of Chinese APT Volt Typhoon targeting US critical infrastructure. Assessments of attacker intent for compromising a network are typically fraught with significant caveats and regularly depend on additional context, including geopolitical factors that shape the relationship between the involved actors. Direct references in the Five Eyes Joint Cybersecurity Advisory to the Microsoft report and the near-simultaneous timing of the publication suggest intensive public-private coordination in advance of the release. Departing from Microsoft's reporting, the Five Eye account does not on the alleged intentions of the Chinese threat actors and instead focuses on the communication of "Indicators of Compromise" (IOCs) and preventive/ mitigation measures. These differences may point to an emerging division-of-labour in the practice of attribution, in which government agencies leave the more politically-charged statements to the private company and focus more on the resilience-building aspect.

Bangladesh also registers notably in the list of countries of origin, with three attributed incidents. The country was not on the list in March or April. This change in May is due to the activities of the hacktivist group Mysterious Team Bangladesh. The group first appeared publicly in 2022 through DDoS attacks primarily aimed at Indian targets. Relations between India and Bangladesh are marred by border conflicts, disputes over important resources such as water, and religious animosities.

Such a convergence of tensions makes patriotic or ideologically-motivated hacktivist operations more likely and may explain the concentration Indian targets. This nexus to political grievances is less apparent in more recent activity. In 2023, the group shifted its focus to primarily Ethiopian and Senegalese institutions, as captured in two of the three incidents recorded in May. No specific openconflict or dispute between Bangladesh and the countries is publicly known, which may also less seem likely due to the geographical distance. Hacktivist attacks tend to be directed against regional rivals of a group's home country and less often against countries of other regions, unless they act in support of hostile states. Considering these factors, the activities of Mysterious Team Bangladesh may be an opportunistic attempt to demonstrate the group's own capabilities and generate attention by striking insufficiently protected targets.

Significantly fewer operations were attributed to Russia's war against Ukraine, with 7 incidents recorded in May; in April, there had been 15 incidents. Three of the operations involved states that support Ukraine (Italy, France, and the Netherlands). Based on public reporting, DDoS operations by pro-Russian hacktivist groups, such as the NoName057(16) group, remain the main type of incident affecting Ukraine's international partners. Geopolitical tensions between Iran and Israel were the political context that recorded the second most frequent attribution of cyber incidents (4 incidents). Iranian APTs consistently target their operations to capture sensitive information from public and private Israeli institutions. In one case, the group Agrius disguised its operation as an alleged ransomware operation, an increasingly common tactic used by state-sponsored groups to cover up destructive, politically-motivated attacks.

More from EuRepoC

In a working paper published in early June by EuRepoC consortium member Stiftung Wissenschaft und Politik, Mika Kerttunen addressed the question of the extent to which the use of military cyber capabilities already constitutes a state of war from a military-theoretical and operational perspective. The current use of cyber operations in the context of the war against Ukraine is discussed in particular.

EuRepoC also 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