European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

June 2023

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

Overall observations

In June 2023, 75 cyber operations were recorded in the **EuRepoC database**. This is a 33% decrease compared to the previous month but 22 operations above the average recorded activity of 53 cyber operations per month.

The **average intensity** of operations recorded in June 2023 stood at 2.89, exceeding the historical average of 2.6. 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.

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.

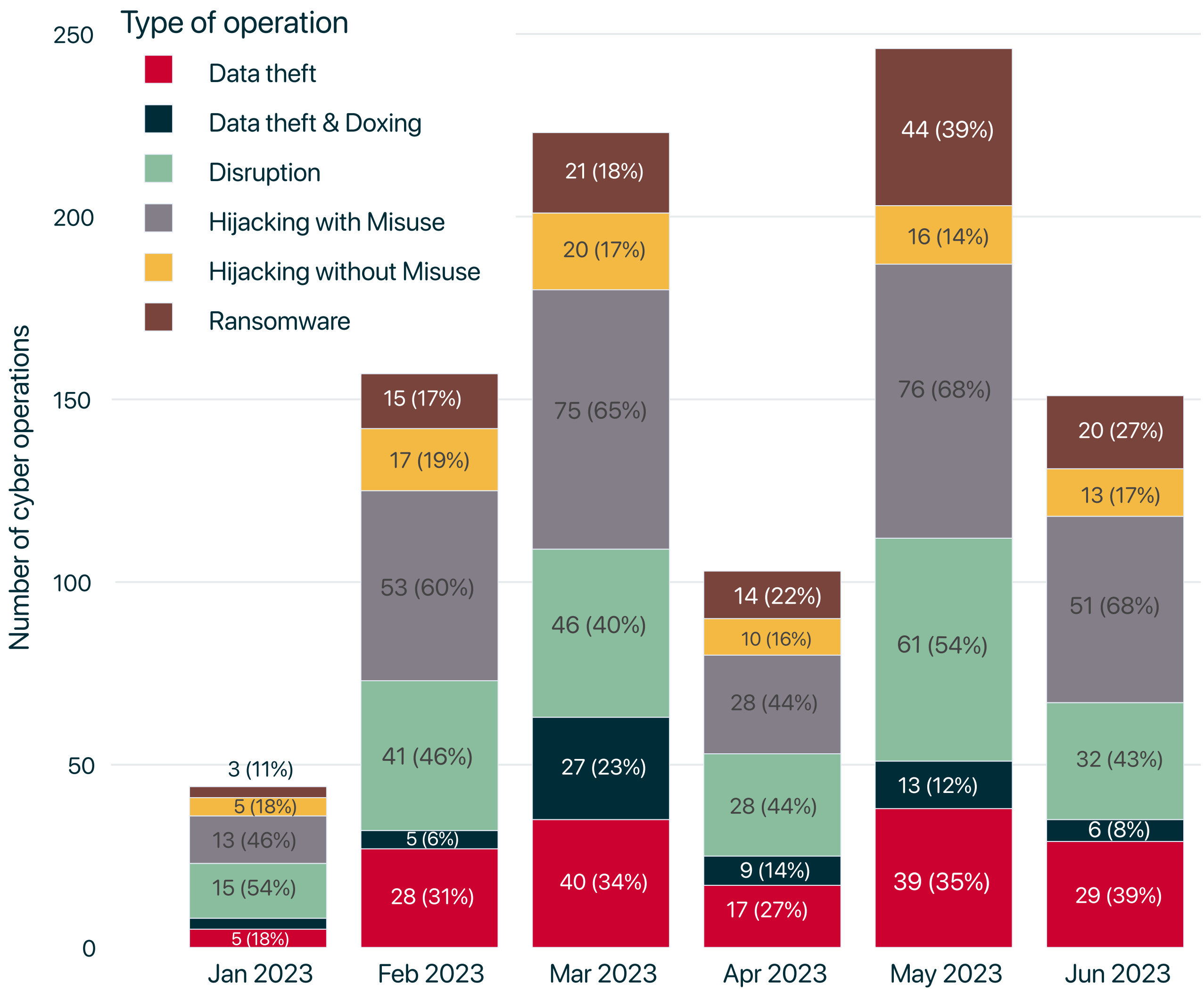
About EuRepoC

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 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 activity tracked in June comprises "hijacking with misuse" operations (68%). 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, identifies data theft or operational disruptions.

A particularly sophisticated example is the use of the spyware "Triangulation," as reported by the Russian IT security firm Kaspersky.

The espionage tool was implanted onto the iPhones of Kaspersky employees, among others, by exploiting a so-called zero-click mechanism (further details on the assessment of the incident by the Russian domestic intelligence service FSB can be found in the "Threat actor profiles and attributions" section of the briefing).

Zero-click exploits are primarily used against and can infiltrate mobile devices without direct user intervention (hence the name "zero-click"). In normal use, they are therefore virtually undetectable, especially if access is established via vulnerabilities not previously known (zero days). A notorious example of this method is the Pegasus program, which was commercially distributed by the Israeli spyware company NSO Group.

Zero-click vulnerabilities are noticeably rare even among zero days that are already considered valuable assets. This remains true even as security researchres have come to refer to Summer 2023 as the “Zero-Day Summer,” a tongue-in-cheek recognition of the frequent observation of exploited new security vulnerabilities (one example in this context is the vulnerability in the MOVEit file transfer platform mentioned in the “Focal points and targeting patterns” section of this briefing). The Triangulation spyware leverages several of these zero-day vulnerabilities. As of 24 July, Apple had fixed three zero days on Kaspersky's advice. A possible fourth vulnerability had already been closed in December.

"**Disruption**" operations accounted for the second-most common type of operation recorded in June. These are operations aimed at putting an information technology service out of operation. A disruption operation thus affects its availability. The majority of disruption operations are typically temporary in effect. In June, EuRepoC recorded 32 such operations.

Examples include ransomware attacks, such as that against the Swiss IT company Xplain, which are launched with the intention of forcing companies to pay a ransom by encrypting business-critical data or threatening to publish trade secrets. Xplain specializes in developing software solutions for internal security. Customers include national and cantonal authorities, such as the Swiss Federal Office of Police (fedpol).

According to preliminary assessments, government data was not the direct target of the attack. Nevertheless, the ransomware group "Play", which is presumed to be responsible, managed to gain access to classified and sensitive documents via Xplain.

A small portion of the 400 GB of data leaked by Play includes operational data of potentially high consequence.

For example, some documents contain fedpol information on security measures for 63 diplomatic missions and Swiss government facilities, along with threat assessments and the home addresses of several cabinet members. Reflecting the state of play from 2017/2018, the information was passed to Xplain as sample data, although classified, to aid the company in structuring data outputs.

Analysis of the extensive dataset is time-consuming. Media reports differ accordingly as to whether the information from Interpol contained in the dataset concerns active arrest requests (Red Notices) or their suspension.

Sources in the federal administration, meanwhile, confirmed the publication of Swiss arrest warrants and interrogation protocols. For this reason, among others, the Federal Data Protection and Information Commissioner opened an investigation against fedpol on the initial suspicion of potentially serious violations of data protection obligations.

Based on claims by the ransomware group, the published files so far comprise just under half of the total 907 GB of data stolen. Accordingly, it cannot be ruled out that the group withheld information for sale at a later point after it became clear that Xplain - according to the Swiss National Cybersecurity Centre - would not comply with the ransom demands.

An administrative investigation set up by the Swiss Federal Council will look into Xplain's implementation of the regulatory security requirements. This case also raises the question of how public agencies can exercise their due diligence responsibilities with respect to contractors regularly and independently of incidents, and how compliance with security standards and data protection agreements can be verified.

Security requirements that mandate the use of domestic suppliers, as in the Swiss case, may concentrate risks in the systems of a small number of companies in countries with a limited number of domestic market providers. Under these conditions, government contractors could be identified even without major reconnaissance efforts.

According to the Swiss intelligence agency NDB, Switzerland has one of the highest numbers of Russian intelligence operatives active under diplomatic cover in Europe, in part because of its role as a host state for international organizations.

In a newly-published situation report, the NDB underscores this assessment by pointing to an increase in the combination of attack vectors through which foreign intelligence services are attempting to merge intelligence obtained through digital and analogue means.

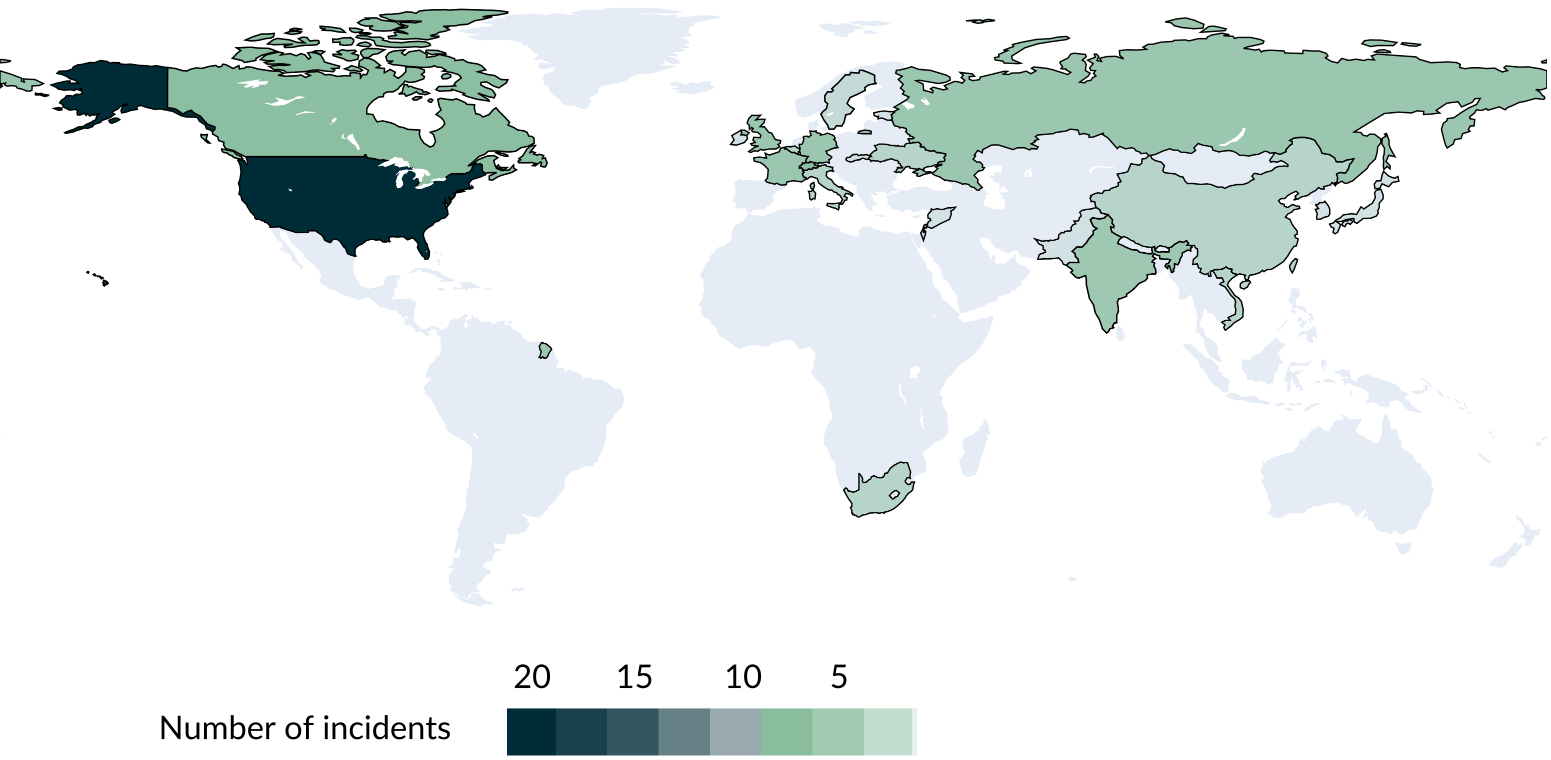
Against this background in particular, insights into the protection plans for diplomatic institutions have a high information value for foreign intelligence services.

Focal points and targeting patterns

The most frequently targeted sector in June, as in the previous month, was critical infrastructure, with 45 cases, or about 60% of new recorded cases. This represents a decrease of about one-fifth from the number of cases in the previous month (56 cases). Government institutions were the second-most frequently affected, with 33 cases (44%), again a decrease of 40% in line with the overall trend.

In line with the distribution of previous months, the United States was the most frequently affected country, accounting for almost 30% of all cases (22) and reflecting the country's global weight in the adoption and development of networked technology. Next-most targeted were European countries: Switzerland, Germany (six cases each), and France. Among the total of 18 cases involving member states of the EU, Germany thus accounted for one third, which in absolute terms corresponds to the quantity of the previous months.

Geographic distribution of operations



The number of new incidents recorded for Switzerland stands out at first glance. Given the nation's politically neutral position in the war against Ukraine, "spillovers" of cyber activity related to the conflict might seem less likely. A closer look reveals a different picture: On the occasion Ukrainian President Zelensky's virtual address to the Swiss National Council on 15 June, several distributed denial of service (DDoS) attacks by Russian vigilante groups targeted websites of Swiss authorities and transport companies, similar to hacktivist activitiy drawn by other European states in recent months in response to decisions seen as supporting Ukraine, such as arms deliveries (see EuRepoC analysis for further details). The aforementioned ransomware incident at the software company Xplain, which led to the publication of sensitive documents, was technically much more elaborate but based on preliminary assessments not tied to the political context of the war against Ukraine.

With the exception of the compromise of email accounts of the German Social Democratic Party, a hack attributed to Russian groups, the incidents affecting Germany were also without any discernible political connection and concerned, for instance, ransomware cases at the Hochschule Kaiserslautern, as well as at several banks as a result of a critical security vulnerability in the file transfer software MOVEit, and the Bremen-based hospital group Gesundheit Nord.

Sector-wise, the incident at Gesundheit Nord represented one of 16 recorded cases in which healthcare facilities were affected as part of critical infrastructure targeting. The healthcare sector thus continues to be one of the critical infrastructure verticals most acutely affected, as already described in the EuRepoC briefing for April.

In many cases, questions about the responsibility for attacks remain unresolved. In some instances, however, IT security companies or governments have published indications of the possible regional origins of the operation (but not necessarily of government responsibility).

Threat actor profiles and attributions

In June, cases for which responsibility had not yet been publicly determined made up the majority of database entries (51). At 68% of the total recorded incidents, this is almost as many in relative terms as in the previous month (70.5%).

For attributed incidents, threat actors were most frequently identified as operating from Russia (14 reported operations). In contrast to May, no Iranian groups were tracked for June. Chinese groups were identified as responsible for three incidents in a tie with North Korean threat actors in terms of the number of conducted operations. Although Vietnam and India, two countries for which no attribution was recorded in May, were referenced in June, the pool of attributed attacker countries of origin was noticeably smaller for June.

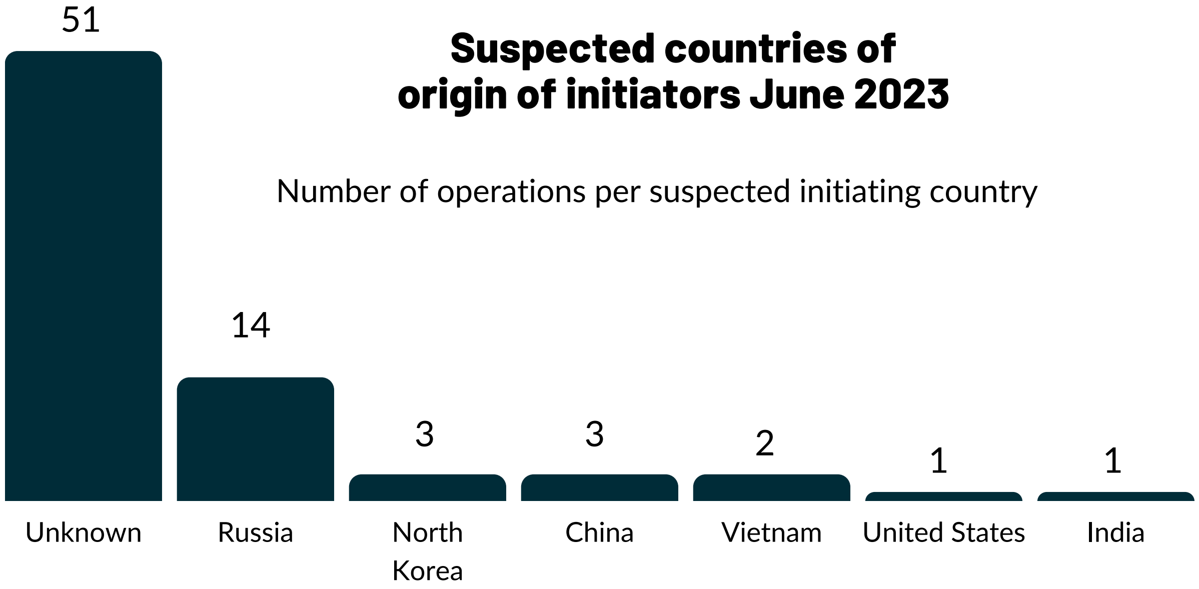
29 of the 75 incidents in June were attributed to non-state actors (including state-affiliated actors), largely accounted for by the continuously high level of ransomware incidents linked to criminal groups (13) as well as politically motivated hacktivism (7 entries).

In comparison, cyber operations at the level of political significance tracked by EuRepoC rarely are conducted by single individuals, as both state-sponsored actors (APTs), professional criminal outfits and hacktivists require the resources of a group of operators. Accordingly, in June, only one case of data theft was tied to a still unknown perpetrator who, among other things, had stolen patient data from a medical laboratory in Naples. Here, too, however, further investigation might prove that several people were responsible for the operation.

Of particular interest is the sole incident attributed to the United States as the attacker's country of origin: On 1 June, Russia's domestic intelligence service, the FSB, accused the US National Security Agency (NSA) of spying on the iPhones of several unnamed Russian users and diplomats from various countries working in Russia. The Russian authorities did not specify the period for which they had observed the intrusion.

The statement also, without providing evidence, accused Apple, of cooperating with the US intelligence community, insinuating that the company had provided information about vulnerabilities or left known weaknesses unaddressed - claims that the iPhone manufacturer flatly rejected.

Notably, the Russian threat intelligence company Kaspersky published a report on a related set of activity dubbed "Operation Triangulation" (referred to earlier in this briefing) on the same day as the FSB statement. As confirmed via Twitter by Kaspersky researcher Ivan Kwiatkowski, the report describes the exploitation of the same vulnerabilities that underlie the FSB allegations and a subsequent alert issued by Russia's government CERT.



As noted, "Operation Triangulation" was carried out by spying on iPhones using zero-click exploits, reportedly also affecting the smartphones of senior Kaspersky employees even though Kaspersky assesses the company not to be the primary target of the operation. Based on the timeline, as well as the associated media coverage, it may seem plausible that this represents a case of coordinated public-private attribution, similar to the simultaneous reports from Microsoft and Five Eyes agencies on critical infrastructure intrusions associated with the Chinese APT Volt Typhoon, about which EuRepoC reported in the May briefing. Conjectures in this vein are challenged, by the statement of Igor Kuznetsov, a senior researcher at Kaspersky, who noted the company had not coordinated with the FSB in advance and was surprised by the agency's statement. A functional comparison of the FSB and Kaspersky reporting in the present case shows further differences, in that Kaspersky as a private-sector threat intelligence company published only technical evidence while political attribution of responsibility was undertaken by government agencies. The nature of the reports follows the respective reputation and credibility status of the actors. Whereas Kaspersky continues to operate as an internationally active and successful IT company despite repeated warnings about potential Kremlin influence over the company, the FSB is unlikely to lose (or gain) credibility with an international audience as a result of a public attribution of responsibility to the United States. Drafted in Russian, the FSB's assignment of responsibility may also have been principally directed at the domestic population to signal detection and attribution capability in times of armed conflict. Published in English, Kaspersky's analysis is more easily accissible to a broader international readership.

In June, EuRepoC registered a first incident involving APT DoNot (also tracked as APT-C-35), a group suspected to operate from India. A growing number of APT groupings has been attributed to India as a country of origin. The best known among these are the APTs Patchwork (aka Dropping Elephant), BITTER, and SideWinder. Their actions have so far been primarily directed against Pakistani targets, but as in the case of BITTER have also targeted Chinese entities, including organisations within the nuclear energy sector.

While Kaspersky considered indicators for SideWinder's connection to India to have weakened over time (May 2022), a comprehensive report by Group-IB (February 2023) highlighted links between SideWinder, Patchwork, and DoNot, suggesting internal cooperation, or potentially sharing of technical tools and infrastructure, among Indian APTs, similar to the case of many Chinese APTs.

Of the 75 incidents for which attribution information was collected in June, 11 were linked to existing conventional conflicts. In a hardening pattern, Russia's war against Ukraine and related cyberattacks by both sides dominated, totaling six operations. Two other dyads of so-called "enduring rivals" ranked second and third: the conflict between North and South Korea (2 cases) and between India and Pakistan (1 case). Although cyber operations are not physically tied to territorial borders, and may often produce impact across borders, as an extension of regional conflicts cyber activities regularly show a certain physical proximity of the conflict parties.

More from EuRepoC

In July, EuRepoC researcher Kerstin Zettl-Schabath published her dissertation "State Cyber Conflicts: Proxy Strategies of Autocracies and Democracies in Comparison" with Transcript-Verlag. In it, she compares the autocratic and democratic use of cyberproxies by China, Russia, the US, and Israel drawing on the Heidelberg cyberconflict dataset HD-CY.CON, upon which the EuRepoC database is built.

EuRepoC researchers Jakob Bund and Annegret Bendiek chronicle the deliberations by a growing number of states concerning the adoption of an active cyberdefense posture in a new policy paper that ponders the implications of such a "Paradigm Shift for European Cyber Defense". Analysing existing and proposed efforts to disrupt malicious cyber activity before it can cause harms, the paper emphasises the need to democratically anchor discussions of these measures - to ensure that, where adopted, they reinforce responsible state behaviour. The German edition of the paper is available from the website of the German Institute for International and Security Affairs (SWP).

In addition, EuRepoC provides information about new cyber incidents added to the database with 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