European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

March 2023

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

Overall observations

March 2023 was a noteworthy month in terms of cyber operations recorded by EuRepoC. During this period, 88 cyber operations were recorded in the database. This is 12.82% more than the previous month and 51 operations more than the average recorded activity of 37 cyber operations per month.

The **average intensity of operations** recorded in March 2023 is 3.1, which exceeds the historical average (2.4). The striking increase in operations since February 2023 can also be explained, above all, by the fact that EuRepoC is recording all cyber attacks against critical infrastructure targets from March 2023 onwards 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 March, but may have started earlier. The focus is on technical, political, and legal aspects.

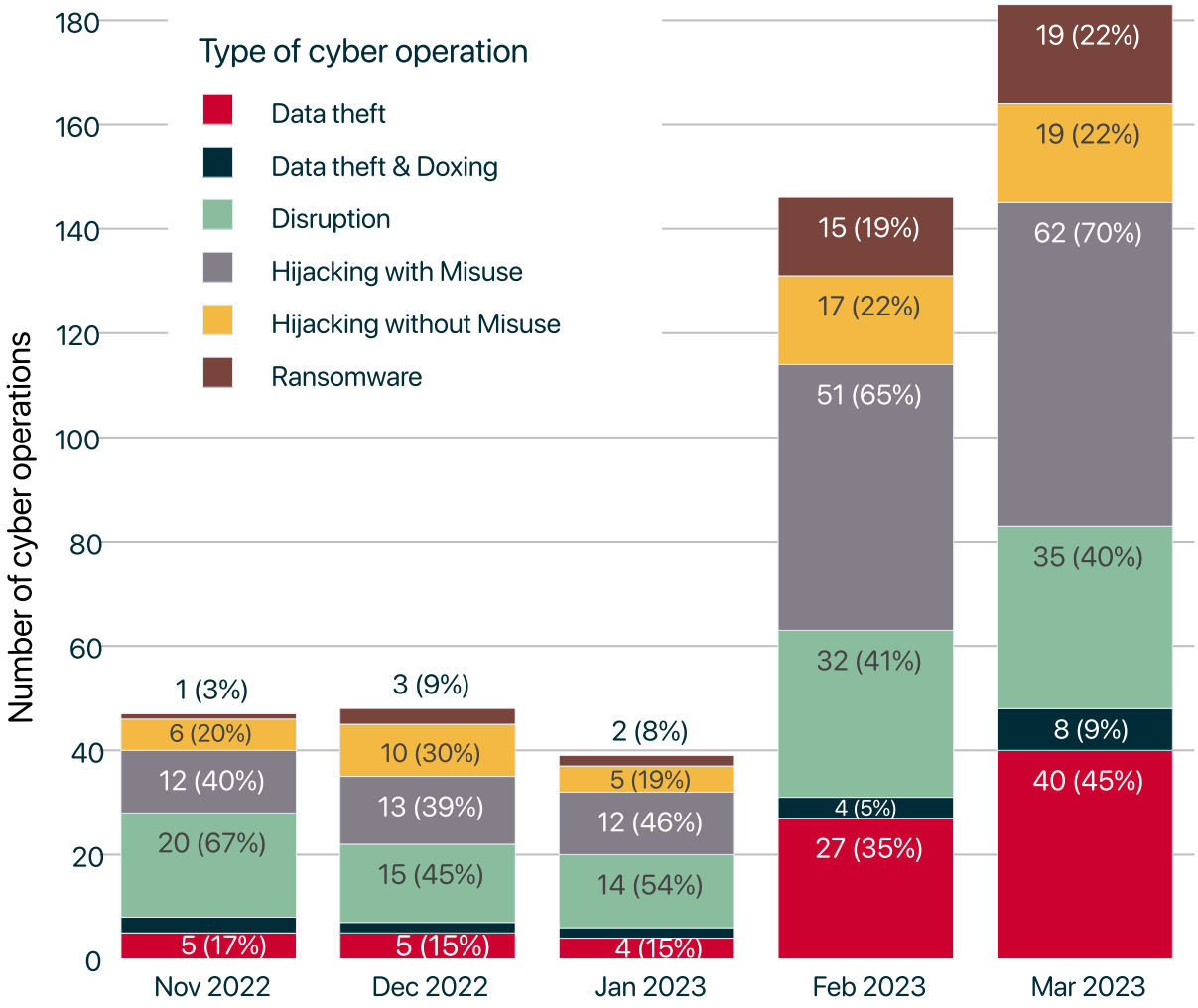
About EuRepoC

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 March 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 comprises "**hijacking with misuse**" operations. As a collective term, these are operations in which attackers have succeeded in penetrating systems and networks to carry out unauthorised, harmful actions. Under certain circumstances, these actions also allow initial conclusions to be drawn about motives, e.g., if they are carried out specifically to cause operational disruptions or to steal data. For March, EuRepoC documented 62 such operations.

One example is a recorded intrusion into the networks of a US federal agency by the criminal unit XE Group, which is suspected of operating from Vietnam. The attackers gained access via a user interface vulnerability that had been known since 2019 because an incorrectly configured vulnerability scanner did not report the vulnerability. As early as 2020, the National Security Agency had explicitly warned about the vulnerability and included it in a top list of software flaws regularly exploited by Chinese state-backed hackers.

As such, the case illustrates the **longevity of critical vulnerabilities** even in high-value targets despite active efforts to render them harmless. In the course of advancing digitalisation, this case also exemplifies the complexity of these efforts, given i**ncreasingly multilayered network architectures** and **growing dependencies** on external software providers.

The second most common type of operation was **data theft**. The aim of these operations is to acquire data or information without permission. Although the data is not automatically "lost" to the target, it loses its confidentiality if it is not publicly available. Data theft can be based on political, financial, economic, or personal motives. Incidents involving state actors are usually reported under the heading of "**cyber espionage**." EuRepoC has recorded 40 such incidents.

This is exemplified by reported espionage operations against the Association of Southeast Asian Nations (ASEAN) in early March, in which **Chinese threat actors** captured more than 10,000 messages from one of the organisation's email servers. The stolen messages provide insight into internal deliberations on economic integration, infrastructure projects, and trade talks. Although a cybersecurity alert was sent to the relevant authorities of the ten ASEAN member states shortly after the theft was discovered in February 2022, the case was not publicly acknowledged until a little over a year later.

According to this warning, **ASEAN** has been the focus of Chinese hackers in at least three independent espionage campaigns since 2019. The case thus illustrates that even recurring attack patterns sometimes only become public after a considerable delay.

This dynamic underlines the importance of continuous monitoring and pooling of information in order to assess the combined impact of cumulative actions.

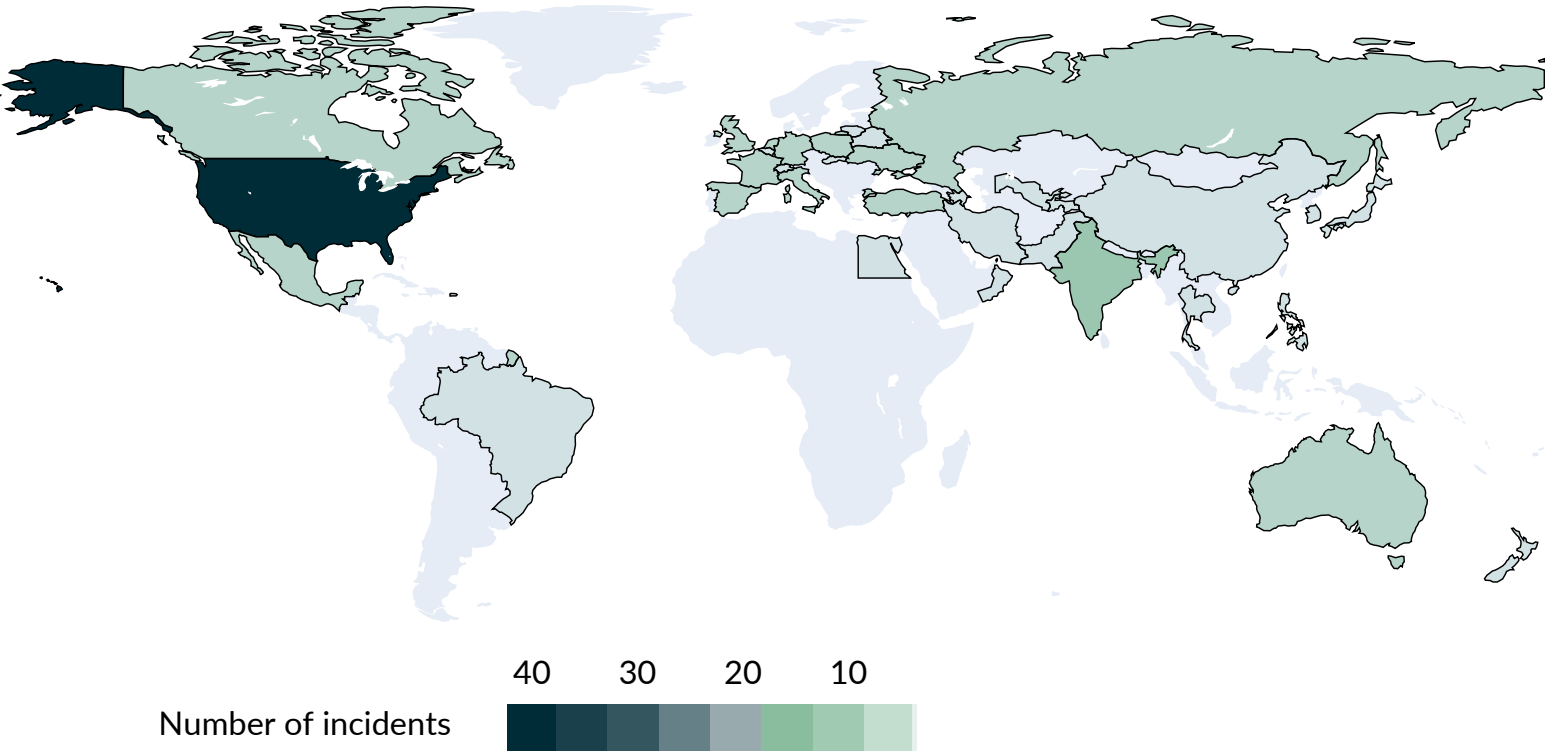
Focal points and targeting patterns

The **affected countries** are distributed across the regions of **North America**, **Europe**, and **Asia** and thus the global north. The database recorded 24 cyber operations (19 of them in EU member states) with targets in Europe and 14 incidents with Asian targets. However, the majority of incidents involved the US (38), reflecting its generally high attractiveness and vulnerability to cyber attacks.

The broader inclusion of **ransomware incidents against critical infrastructure since the beginning of March** allows us to draw a more accurate picture of the threat situation for various sectors from ransomware, even without a political/governmental attack background. For example, almost 70% of the ransomware incidents recorded by EuRepoC in March affected US victims, such as police agencies like the US Marshals Service or the Washington County Sheriff's Office. The health and care sector was also frequently affected, especially in Europe, such as clinics in Barcelona and Switzerland and an elderly care facility in the Netherlands. In the US, for example, the insurance company US Wellness was affected.

This reflects the increased focus of cybercriminals on particular critical infrastructure targets whose potential willingness to pay is likely to be especially high. If a ransomware attack is not only about financial gain, but the attackers also aim at political destabilisation, hospitals or energy plants are equally attractive targets.

Geographic distribution of operations



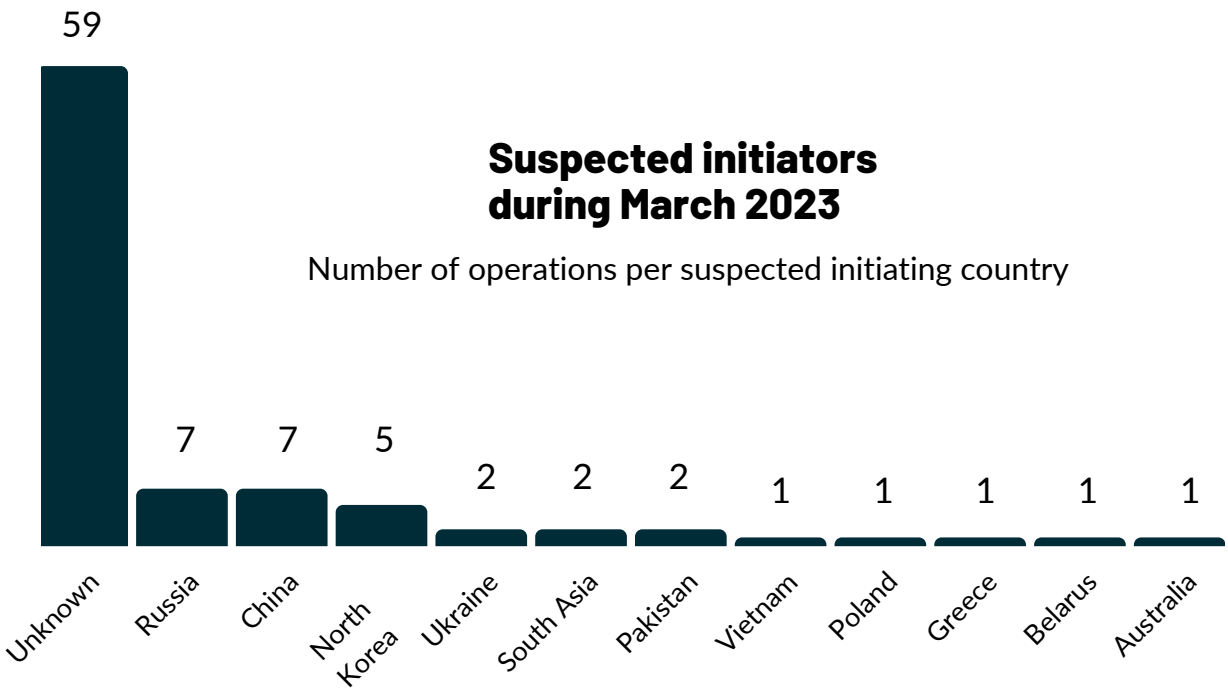
For **Germany**, no ransomware incidents were included in the EuRepoC database in March. Instead, the (short-lived) DDoS attack on the arms company Rheinmetall, the theft of emails from German and South Korean research institutes, which authorities of both countries jointly investigated for the very first time, and at the end of the month, the cyber incident at the local transport company Üstra in Hanover marked noteworthy events.

The **most frequently-targeted sector** in March 2023 was government/political institutions or actors, with 67 cases, compared to the previous month, when critical infrastructure was the most-targeted, with 86 cases.

In many cases, the attribution of **initiating actors** is still unfolding. In some cases, however, IT security companies or governments have published references to the possible regional origin of the operation(s), but not necessarily to state responsibility.

Threat actor profiles and attributions

There are hardly any surprises in the list of the most frequently-recorded attacking countries: Chinese and Russian hackers are particularly high-profile and have been responsible for many cyber incidents in the past; the same applies to third-placed North Korea. It is noticeable that, in the month of March, Iran is missing from the list of attackers; Iran normally follows closely behind Russia and China together with North Korea.



The possible reasons for this can be multifaceted: Possibly the attacks were not (yet) detected or not yet attributed to Iranian groups, or they might not have met any of the EuRepoC inclusion criteria.

In addition to attributed operations, however, cases that could not (yet) be attributed to a specific country or actor dominated in March, with 67.05% of cases (59). Particularly for more technically-sophisticated operations (which are often discovered late), a reliable attribution statement usually requires a great deal of lead time for in-depth analysis, which is why many cyberattacks can sometimes only be attributed after several months or even years, if at all. Of the 88 cases recorded, 28 were attributed to non-state actors, which is also related to the increased hacking activities of so-called "patriotic hackers" and "hacktivists" in the context of the war against Ukraine.

Among the attributions recorded in March, the following stood out: on 16 March, the threat intelligence company SentinelOne published a technical report blaming a lesser-known Russian hacking group called Winter Vivern for an espionage campaign against public and private sector targets in Europe and India that has been ongoing since 2021. SentinelOne based its analysis on publicly-available intelligence from the Polish Central Bureau for Combating Cybercrime (CBZC) and the Polish Computer Emergency Response Team (CERT), among others, which once again underscores that attribution of cyberattacks is often a lengthy and cumulative process that requires breaking down individual data silos between attributing actors.

The second notable attribution was the Joint Cyber Security Advisory by the German Federal Office for the Protection of the Constitution and the South Korean intelligence service on 20 March, which described an espionage campaign by the North Korean APT Kimsuky against German and South Korean research institutes.

The Joint Advisory between the two countries is the first of its kind and underlines the increasing cooperation between countries on the attribution level, even across continents. Thus, forces can be pooled, information can be shared, and attribution of responsibility can be given even greater credibility and reach.

Another attribution from 20 March joins the now long list of espionage allegations against European intelligence services accused of misusing NSO Group's Pegasus surveillance software. In this recent example, Greek authorities allegedly spied on a Meta employee using Pegasus during her time in Greece throughout several months in 2021.

Most recently, on 21 March, a technical report by Russian threat intelligence company Kaspersky reveals that new, not previously-identified APTs continue to be discovered. For example, the previously unknown APT Bad Magic used a backdoor to spy on Ukrainian targets in Donetsk, Luhansk and Crimea from late April 2022.

In March 2023, 9 cyber incidents were also attributed to the conventional conflict between Russia and Ukraine, which underlines the still-high level of activity of both pro-Ukrainian and pro-Russian hackers. Even though the attacks by hacktivists are largely low-level, such as the suspected pro-Russian DDoS attack on the German arms manufacturer Rheinmetall on 7 March, actors outside Ukraine continue to face numerous cyberattacks due to their support for the country.

Cyber conflict dynamics related to Ukraine

Since March, EuRepoC has published a detailed profile of the NotPetya campaign from 2017 as part of the new Major Cyber Incidents series. NotPetya continues to be described as the cyber attack with the greatest economic damage, with disruptive effects in Ukraine, which was initially targeted, alongside numerous other countries. NotPetya is also significant because courts have long grappled with the question of the extent to which the resulting impact equates to war-like consequences, which could thus relieve insurance companies of their obligation to pay.

In addition, a recently-published Spotlight Article unpacks nine central observations on the cyber conflict dynamics to date in the context of the war against Ukraine since February 2022, supported by empirical findings from the EuRepoC database. The focus is also on non-state actors (patriotic hackers, hacktivists, or cybercriminals) and their relationship to Ukraine and Russia, as well as their legal classification.

An assessment of the strategic importance of cyber capabilities and lessons learned since the large-scale Russian invasion of Ukraine substantiates this review. In addition, EuRepoC publishes its Cyber Incident Tracker every day, which informs readers about the cyber incidents recorded in the database on the respective day. You can subscribe to it here.

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu