European
Repository of
Cyber Incidents

EuRepoC
Cyber Conflict Briefing

March 2024

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

Overall observations

In **March 2024**, EuRepoC recorded 71 cyber operations, representing a 33.6% decrease compared to the previous month. This figure exactly matched the overall average in recorded activity of 71 cyber operations per month.

The **average intensity** of operations recorded in March 2024 registered at 2.42, below the historical average (2.8). 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 been recording 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 March, but may have started earlier. The focus is on technical, political, and legal aspects.

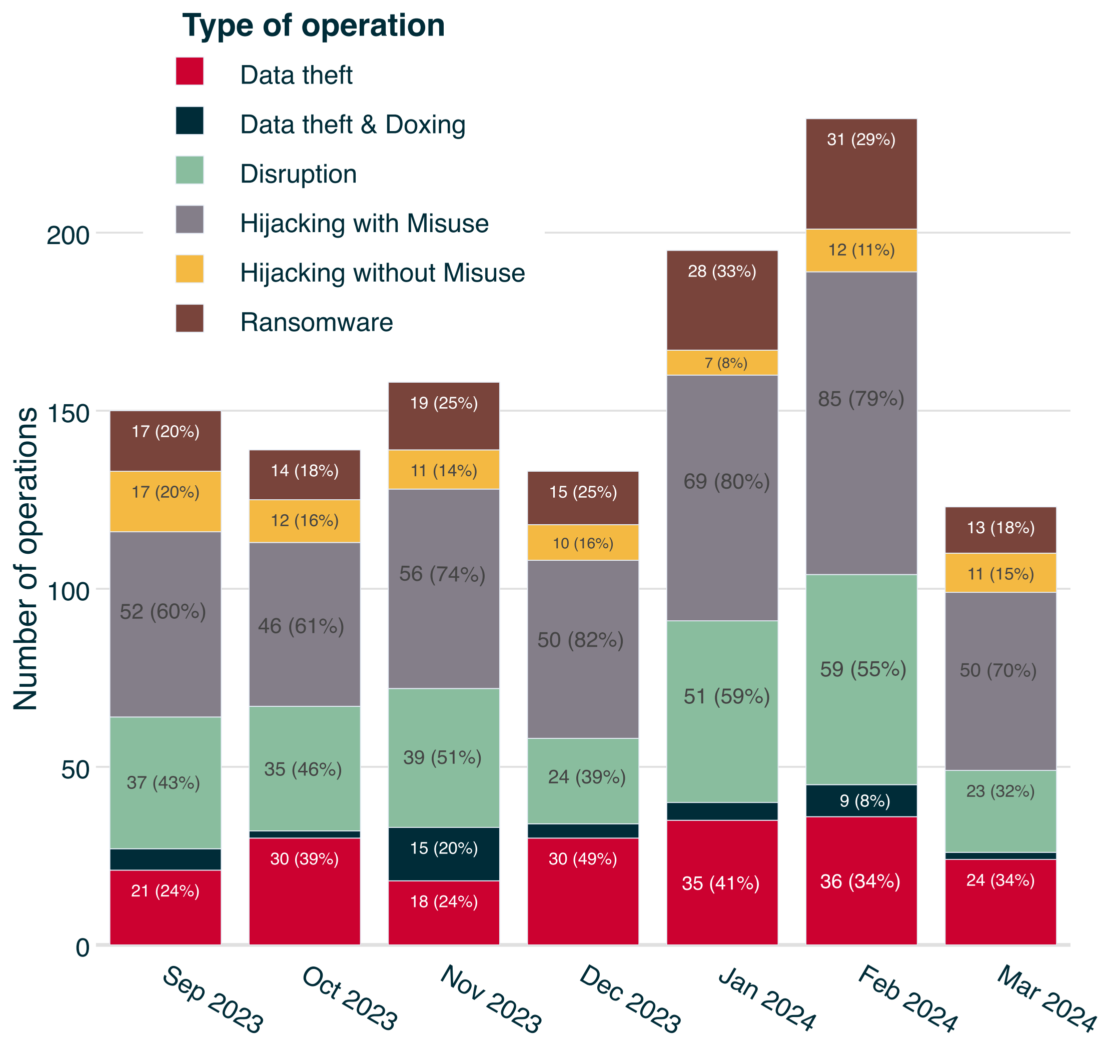
About EuRepoC

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

Monthly distribution of operations



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

In March, the predominant activity observed consisted of **"hijacking with misuse"** operations, comprising 50 cases, which accounted for 70% of the total. As an umbrella term, this describes operations in which threat actors have succeeded in infiltratinh systems and networks to carry out unauthorised, harmful actions. Where feasible, EuRepoC distinguishes these activities based on threat actor intent and, when applicable, identifies data breaches or operational disruptions.

The Czech cybersecurity company Avast, for example, reported a carefully-planned hijacking attempt by the Lazarus Group, which is believed to be controlled by North Korea's Reconnaissance General Bureau. Lazarus used a particularly intrusive, previously-unknown vulnerability to gain access to the kernel level - the core of an operating system that acts as an interface between software and hardware - using a native Windows driver. The driver used for the operation supports AppLocker, a built-in Windows function to whitelist certain software applications.

This attack path directly targets a Windows security building block responsible for enforcing application policies. Exploiting this zero-day vulnerability in an integrated driver allowed Lazarus to gain kernel privileges and execute arbitrary code. This extended access allowed the group to disable security software and directly manipulate kernel objects.

Compromises leveraging this BYOVD (Bring Your Own Vulnerable Driver) technique usually require third-party software to be loaded. In this instance, Lazarus targeted a driver that was pre-installed on the target systems through the operating system. This approach combines BYOVD techniques with "living-off-the-land" tactics to further complicate detection. The bar for carrying out such operations is high, since the number of drivers integrated into operating systems is lower and their code quality typically higher than for other drivers.

To analyse how the vulnerability was targeted, Avast developed a proof-of-concept exploit, which the company submitted to Microsoft in August 2023. Microsoft then provided a patch in February 2024 as part of its monthly update cycle. Avast researchers assessed that fixing the zero-day vulnerability that enables this rootkit blunted one of Lazarus’ most complex tools and may push the group to less well-camouflaged BYOVD techniques. Avast did not disclose details about the victim of the attack or how successful the operation was prior to its discovery.

The second most common type of operation identified in March was "data theft" operations (34%). EuRepoC recorded 24 such operations in March.

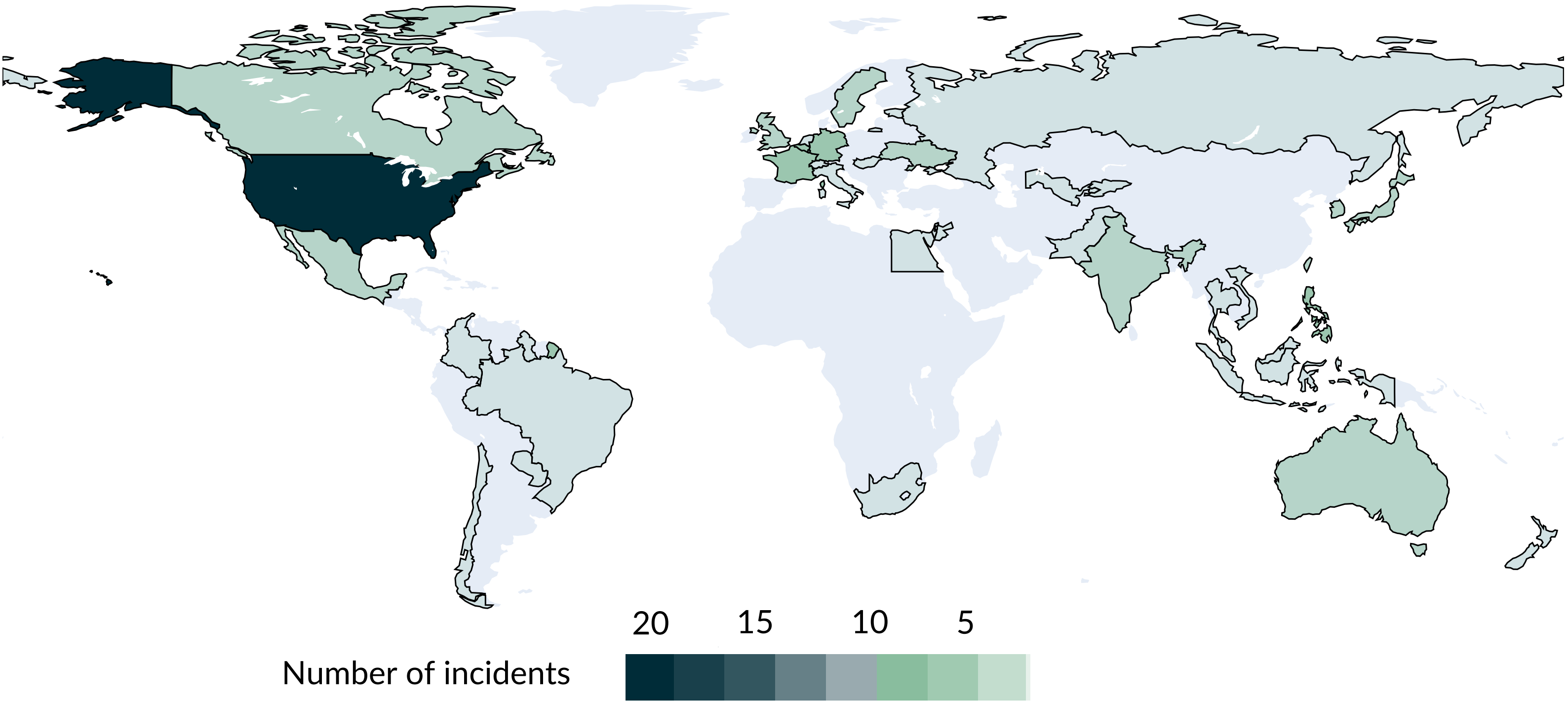
Acer Philippines, a subsidiary of the Taiwanese hardware and electronics manufacturer, was among the companies affected by data theft in March. The unauthorised access to company data occurred in the systems of one of the company's service providers responsible for managing employee data. A threat actor operating under the pseudonym "ph1ns" then distributed a sample of the stolen information via a hacker forum and offered the data set for free download.

In their forum post, ph1ns declared allegiance to the alleged hacktivist campaign #OpEDSA. In a call-back to the EDSA revolution of 1986, a non-violent movement that rebelled against the dictatorship of Ferdinand Marcos and campaigned for democratic reforms in the Philippines, #OpEDSA claims its actions protest against authoritarian structures and economic grievances. Companies operating in the Philippines are a declared target for the group in the endeavour to exert pressure on the country's political leadership.

In this specific case, the responsible actor ruled out negotiations with Acer. Ph1ns stated that they had not attempted to blackmail the manufacturer and provided evidence of the deletion of data from the compromised servers.

This approach emphasises the risks companies face from hacktivist activities in socially-charged situations. The actions of #OpEDSA also underscore the disruptive potential of hacktivist operations, where reversible actions, such as the encryption of important data, are linked to specific political demands.

Geographic distribution of operations



Focal points and targeting patterns

The most frequently affected sector in March 2024 was government institutions, with 36 cases (51% of newly recorded cases), surpassing the critical infrastructure sector for the first time since the Briefings have been published. Critical infrastructure targets were affected in 33 cases (46% of all cases). Compared to February, this represents a reduction in the number of recorded incidents by almost a quarter among state institutions and by a third among critical infrastructure entities. In addition to these two frequently affected sectors, educational institutions were disproportionately affected, being targeted in ten cases (14% of the total number), consistent with observations for February.

According to the tracked reports, the United States remained the most affected country with 22 incidents, similar to the activity level of the previous month.

While EU member states were frequently targeted, the 23 documented cases represent a decrease of more than 40% compared to the previous month. The incidents were mainly spread across France (6 cases), Germany and Belgium (4 cases each), and Sweden (3 cases). Outside of Europe, a cluster of activity was recorded for the Philippines. In addition to a comprehensive campaign attributed to Earth Karang/I-SOON (more details below), the four incidents were connected to the hacktivist activities of #OpEDSA covered above.

Among the incidents directed against state institutions in March, around a third can be attributed to politically- or financially-motivated DDoS or spamming campaigns, such as those observed against the Philippines. In Germany, such DDoS attacks targeted the city of Fürth, which faced two incidents in March in short succession.

In Europe, Estonian, Luxembourgian, and Swedish authorities were similarly affected. In one instance, criminals actors briefly gained control over the private Instagram profile of Italian Prime Minister Giorgia Meloni and promoted a Bitcoin scam.

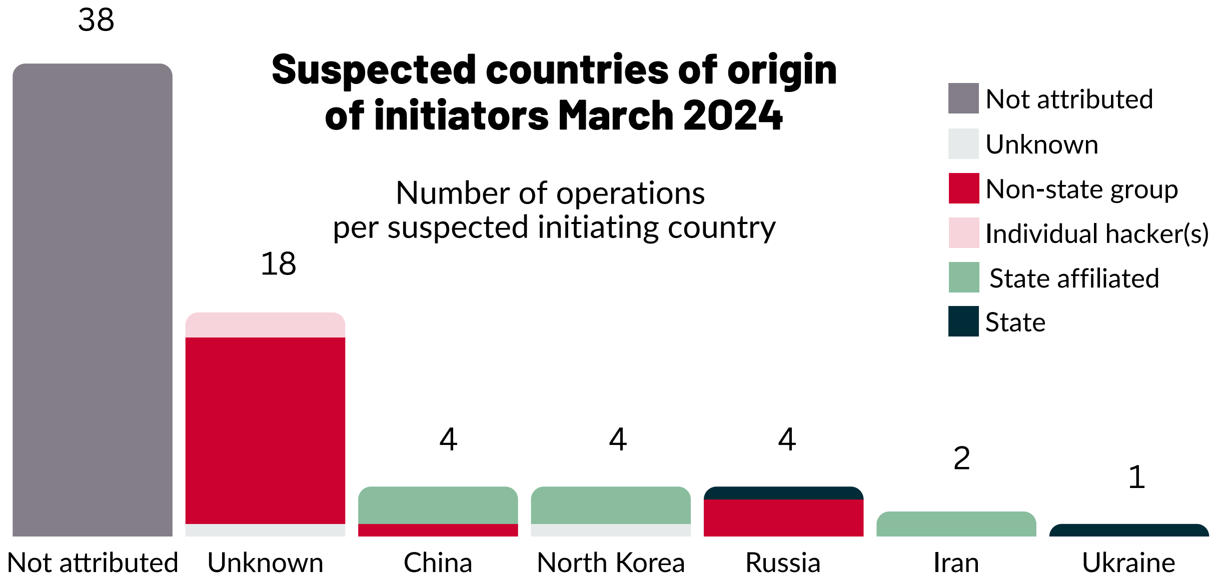
More significant in terms of potential damage was a data theft at the French employment agency France Travail, in which personal information of up to 43 million people was stolen. This marked the second large-scale data breach in France this year, following the compromises of the healthcare payment service providers Almerys and Viamedis that came to light in February. Additionally, a DDoS attack on France's Interministerial Digital Directorate (DINUM), which provides the infrastructure for French ministries, drew considerable attention. Considering the low impact, the subsequent political debate and international reporting was perceived by information security professionals as "exaggerated". Previously-reported vulnerabilities in Ivanti edge devices, which, among others, allowed attackers to gain access to two systems managed by the US cybersecurity authority CISA, remained a focus of threat activity.

As in the previous month, the financial sector was the most affected critical infrastructure sector, with eleven incidents, followed by the healthcare sector with nine incidents. Incidents in the financial sector can be roughly divided into two categories: crypto heists, where hackers for instance exploit vulnerabilities in payment service provider protocols to siphon off funds and data thefts from (US) payment service providers and associated IT service providers. The former typically aim to gain direct access to financial means, while the latter aim to resell stolen data or extort ransom money. Notably, the direct use of ransomware has not been publicly documented for incidents within this vicitimology observed in March.

In contrast, ransomware is deployed in the majority of incidents recorded for the healthcare sector. Criminal groups seek to seize the sensitivity and special legal protection of healthcare data as a means to exert pressure on targets, as affected organisations may not only face a loss of reputation but also significant regulatory fines.

Threat actor profiles and attributions

March saw a nearly identical proportion of unattributed cyber incidents (54%) as the previous month (53%). At the same time, the proportion of operations linked to at least an attacker type, even with country of origin publicly identified, rose from 19% to 25%. In February, the transnational law enforcement action "Operation Cronos" had contributed to a more extensive and diverse list of countries of origin compared to most months on record. Following this deviation, the list of recorded countries of origin for the incidents added to the EuRepoC database in March resembles earlier patterns. Consistently active countries re-emerged, including autocracies such as Russia, China, North Korea and Iran, but also Ukraine, which has been engaged in efforts to counter Russia’s aggression. Accounting for Operation Cronos, the list of countries of origin for March nonetheless appears focused on a small set of states, considering that India and Turkey, but also Vietnam and Pakistan have demonstrated active cyber programmes.



Suspected countries of origin of initiators March 2024

Number of operations per suspected initiating country

This finding appears to be related to the comparatively lower number of total cases in March, a trend also observed in some months of 2023. During those months, the four proactive autocracies—Russia, China, North Korea, and Iran—were primarily responsible for cyber operations in periods with relatively low case numbers.

The proportion of cyber operations attributed to non-state actors (e.g., hacktivists, cybercriminals, or individual hackers) fell by 5% to 21 cases in March. Criminal actors were responsible for 11 of these operations, representing 15% of the total sample, slightly down from 17% in February. Ideologically or politically-motivated hacktivists were recorded in six cases in March, marking a decline from 13% to 8% compared to February. In contrast, the proportion of so-called "proxy operations", i.e., carried out by state-affiliated actors, rose from 6% to 11% in March. The most frequent source of attribution in March was self-attribution, accounting for 21 cases. Threat intelligence companies lead statistics for third-party attribution, with eight incidents included in the dataset in March based on industry reports.

In five cases, attribution of responsibility came from political or state actors in the affected country. The format of these political attributions varies. Communications to this effect may take the form of statements in media reports or short press releases on ministerial websites. Notably, one of the five state attributions occurred in the context of a criminal prosecution by the US Department of Justice. In an indictment unsealed on 29 February 2024, the DOJ published the name of an employee of an Iranian front company, Mahak Rayan Afraz (MRA), which, according to the indictment, carries out hacking operations on behalf of the Islamic Revolutionary Guard Corps. The defendant, Alireza Shafie Nasab, was accused of having been involved in compromising networks of US government organisations and private companies (including in the defence sector) between 2016 and April 2021. On 16 February of this year, the US State Department offered a $10 million reward for significant information about Nasab under its "Rewards for Justice" programme.

These sequenced, and in some cases consecutive, measures by different state authorities against a single individual, each with different objectives and mechanisms, illustrate the increasingly widespread use of "whole-of-government" tools in response to cyber threats. US government responses in particular draw on cooperation between different authorities and agencies, not only in the context of attribution declarations but also in the preparation, coordination, and implementation of efforts aimed at the disruption of threat activity. The indictment against Nasab was followed on 23 April by legal action against three additional defendants: Hossein Harooni, Reza Kazemifar, and Komeil Baradaran Salmani, also from Iran. The group was charged in relation to hacking operations that Nasab had first been accused of. The two months time difference between the separate indictments in February or April suggest that additional findings may have made it possible to identify and bring charges against other members of the group. Procedural or tactical factors may additionally have influenced this approach, considering that the charges in both cases were filed in the Southern District of New York by the same prosecutor.

The case also underscores the existing system of Iranian companies competing for state hacking contracts and, in this role, entering the focus of US investigators. This proxy model shares similarities with Chinese contractors hired by the People's Liberation Army and the Ministry of State Security (MSS), developing a domestic base of companies involved in offensive tooling and driving up competition for state contracts. An extensive leak from the Chinese company I-SOON at the end of February outlined these dynamics in the open.

This leak revealed the considerable scope of activities by a single contractor for Chinese authorities in the hacking and surveillance sector. It also highlighted the challenges these companies face in securing sufficient contracts to remain in business, leading to extensive advertising of their capabilities to potential clients. Notably, I-SOON also collaborated with the Chinese Ministry of Public Security (MPS), which primarily handles domestic surveillance (espionage operations against overseas targets are largely under the direction of the MSS). The competitive environment raises concerns about contractors engaging in financially motivated operations, including ransomware, to buoy up their finances in the event they are unable to secure government contracts.

In March, the number of cyber operations in the context of Russia’s war against Ukraine increased by two incidents, despite the decrease in the number of total cases compared to February. Of the seven cases linked to this conflict dyad, six were attributed to (pro-)Russian actors or directly claimed by them. The remaining case concerned an espionage operation conducted by Ukraine’s Defence Intelligence against the Russian Ministry of Defence.

More from EuRepoC

In April, EuRepoC released a new **Critical Infrastructure Tracker**. The tracker provides interactive analysis tools for various aspects of cyber operations that affected critical infrastructure entities in Germany, the EU, and other regions globally. This includes information on the targeted sub-sectors, attribution information about threat actors, and the links to existing conventional conflicts.

On 23 April, EuRepoC researcher Jakob Bund, together with Microsoft, presented the possible use of Microsoft Copilot for additional analysis of EuRepoC's cyber conflict data at this year's European Cyber Agora in Brussels.

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