European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

Q1 2026

Kerstin Zettl-Schabath
Jonas Hemmelskamp
Lena Rottinger
Erik Kellenter

Overall observations

In the first quarter of 2026 (Q1), **187 cyber operations were added to the database**. Although this represents a 10% decline from the previous quarter, the volume of incidents has returned to the long-term quarterly average, after a peak in activity in 2025 was observed.

With **45 operations**, the United States accounts for nearly a quarter of all recorded incidents in Q1 2026. This makes it by far the most frequently targeted country. However, despite the start of US-led military operations against Iran on 28 February, there has been no measurable deviation from the long-term quarterly average in terms of operations directed against the US.

Taken as a whole, the number of attacks carried out against EU Member States once again exceeded the level of incidents targeting the United States. With 57 operations, the 27 Member States were affected by one-third of all cyber operations. EU institutions were also affected, which is a rather rare occurrence.

About the briefing

The *Cyber Conflict Briefing* series analyses the key trends and dynamics for cyber incidents recorded by the **European Repository of Cyber Incidents (EuRepoC)**.

As of October 2025, EuRepoC prepares the Briefing on a quarterly basis in collaboration with the **Deutsche CyberSicherheitsorganisation GmbH (DCSO).** The German edition is published in partnership with the **Tagesspiegel Cybersecurity Background,** accessible here.

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

Geographic distribution of operations in Q1 2026

First, it was reported on 30 January that the European Commission's central infrastructure for managing mobile devices had been hit by a cyberattack; the names and mobile phone numbers of some staff members may have been leaked. Second, the ShinyHunters ransomware group stole at least 340 GB from the European Commission's cloud during a supply chain attack on 24 March.

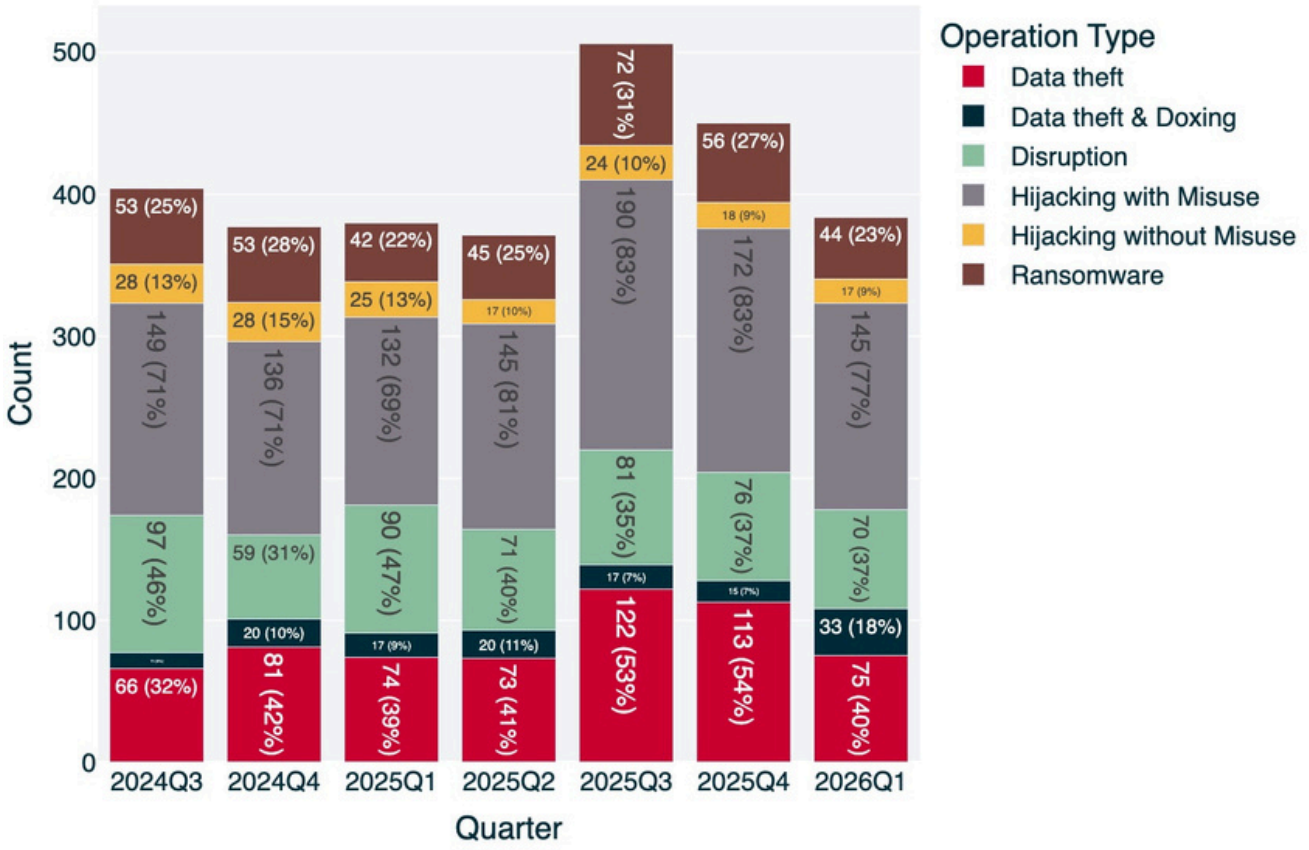
On the national level, France was once again the second-most affected country overall, with 14 incidents. Unknown hackers breached the national bank account database FICOBA and accessed data from 1.2 million bank accounts. Meanwhile, another incident involved the HR software of the Ministry of National Education; personal data of employees in the national education system was leaked. Following France were Germany and Spain, each with 10 incidents. Interestingly, Q1 2026 also saw the first cyber operation targeting Greenland, in which a local bus company fell victim to a DDoS attack.

Focal points and targeting patterns

The relative distribution of operation types remained consistent compared to the previous quarter. The largest share, comprising 144 incidents (77%), fell under the "Hijacking with Misuse" category. This category is typically coded together with other types such as "Data Theft" or "Disruption." In March 2026, for example, several security firms, including Google, announced that a group with ties to the Russian state had acquired two sophisticated iOS exploit toolkits — Coruna and DarkSword — in 2025, both of which had originally been developed by commercial surveillance providers. These tools were deployed against the Ukrainian military sector and critical infrastructure, with the attackers exploiting multiple zero-day vulnerabilities and using novel techniques.

"Data theft" represents the second most common type of operation, accounting for

Distribution of Operation Types



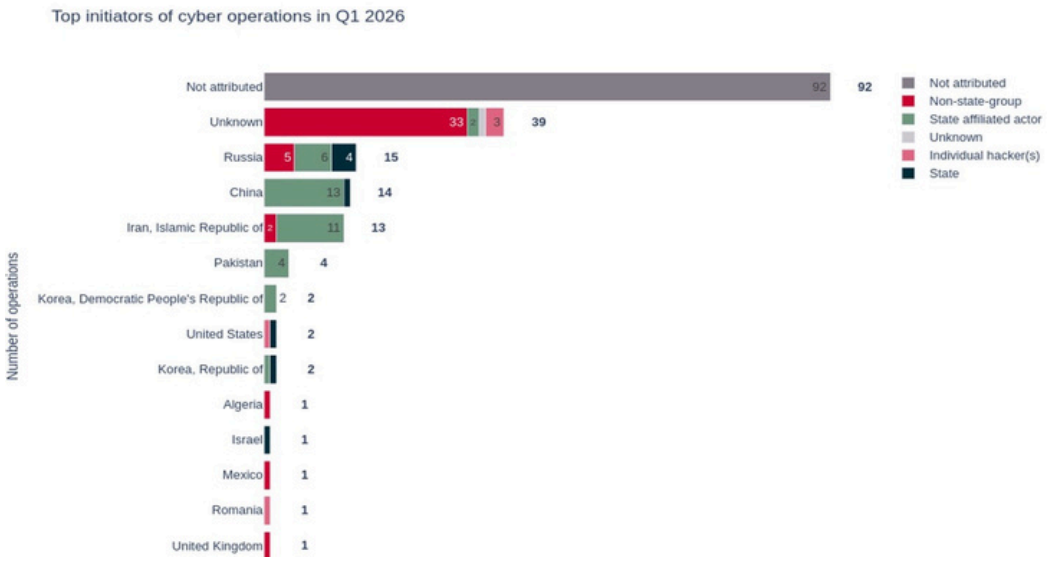
Note: Individual cyber incidents may have several operation types in combination

76 incidents (41%). A separate category, “Data theft & doxing,” covers all operations in which attackers subsequently published exfiltrated data. The relative share of these incidents has more than doubled: from 7% in Q4 2025, “data theft and doxing” increased to 17% in Q1 2026. This observation is likely linked to the increase in cyber operations by Iranian actors targeting Israel and the United States. In this context, data leaks serve, alongside destructive “wiper” operations, as a means of publicly demonstrating cyber capabilities.

Toward the end of March, for example, the Iranian group Handala compromised US FBI Director Kash Patel’s Gmail account and published personal data allegedly obtained from the compromise of that account. The FBI, however, stated that no sensitive government information had been stolen.

Meanwhile, the proportion of incidents involving disruption remained as high as in the previous quarter (37%). However, the proportion of DDoS attacks in this category declined from 20% to 10% despite the conflict with Iran. Over the past three years, the Russia-linked group NoName057(16) was responsible for a large share of all recorded DDoS attacks, but after peaking in 2025, the number of operations attributable to this group dropped dramatically. Consequently, only one DDoS attack was recorded in the last quarter, which occurred during the Winter Olympics in Italy.

Suspected countries of origin of initiators in Q1 2026



Threat actor profiles and attributions

In Q1, most cyber operations originated from Russian, Chinese, and Iranian threat actors. As in previous quarters, certain attack patterns were visible: Russian actors tended to focus on destructive and disruptive attacks, while Chinese actors primarily extracted data and engaged in espionage. EuRepoC also documented a significant increase in cyber activities attributable to hacker groups affiliated with the Iranian government.

In January 2026, media coverage focused primarily on a Russian cyber operation targeting Polish energy infrastructure operators, for which there are several, at times conflicting, attributions. In an official press release, Polish Prime Minister Donald Tusk described the attackers as “groups with direct ties to Russian intelligence services.” He did not specify exactly which groups were responsible for the attack. Shortly thereafter, the Polish CERT (CERT.PL) stated that the attackers’ infrastructure bore a strong resemblance to that of the Russian threat actor “Static Tundra” (aka Bersek Bear, Ghost Blizzard, Dragonfly).

This group had already been attributed by US authorities to the Russian domestic intelligence service, the FSB.

In contrast, the IT security firms ESET and Dragos attributed the attack to the Russian threat actor “Sandworm.” This group was already responsible for successful attacks on Ukrainian energy operators in 2015 and 2016 and possesses a deep understanding of electrical infrastructure. While Sandworm was primarily active in Ukraine for a long time, reports since late 2025 highlight operations in Europe and North America as well. The Polish government has not yet officially blamed Sandworm; the Polish CERT also sees no clear evidence of involvement in this case.

However, all attribution reports agreed on one point: the attackers’ intent was clearly destructive. Had the attack succeeded and actually caused a major network outage, it would likely have had devastating consequences in the depths of the Polish winter.

In addition to Russian threat actors, Iranian actors were also quite active in Q1 2026. Since the start of the Iran conflict on 28 February, EuRepoC has recorded a significant increase in malicious activities directly or indirectly linked to the Iranian government. The attacks were primarily directed against critical infrastructure and government institutions in the US, Israel, and the Gulf States. Europe has so far been largely spared, with the exception of Ireland (where Stryker is located) and Albania.

The purported hacktivist group "Handala" claimed responsibility for about half of the incidents linked to Iran. Among other targets, Handala compromised the major US medical technology corporation Stryker. The FBI subsequently classified Handala as an actor operating on behalf of the Iranian Ministry of Intelligence and Security (MOIS), and the FBI also established a link between Handala and another Iranian entity named "Homeland Justice," which has primarily targeted Albania in recent years.

At the onset of the conflict, several countries, including the United Kingdom and Canada, had already warned of a potential increase in Iranian hacking activities. The US is also stepping up its response to cyber threats from the Iranian government, not only by seizing several domains belonging to Handala, but also by announcing a US$10 million reward for information on hackers working for the Iranian government. In addition, US authorities published several technical advisories indicating that critical infrastructure in the US is being targeted by Iranian hackers.

An analysis of Iranian attacks reveals a clear pattern: state-sponsored Iranian threat actors have developed a new preference for operations that generate greater public attention and are more destructive and disruptive. This stands in contrast to previous Iranian cyber activity, which over the past 25 years has tended to focus on espionage and intelligence gathering. Despite Iran maintaining a comprehensive system of state-run and state-sponsored hacking groups, its actual capabilities in cyberspace have proven to be comparatively limited as the conflict has unfolded.

The conflict also highlighted how Israel and the United States use cyber operations to complement or enhance kinetic operations. This is achieved in part through influence campaigns or by using mobile devices and surveillance cameras for target selection and damage assessment.

Developments in the cybercrime ecosystem

Key observations from Q1 can be summarised as follows:

- In Q1 2026, the open-source ecosystem continued to evolve into a key entry point for criminal and state-affiliated actors. Compromised npm packages, such as those discovered by Axios on GitHub, demonstrate how supply-chain attacks can affect thousands of users. The complex processes, ranging from initial access to downstream attacks, also increase the risk of a lasting loss of trust in the ecosystem. Not only are individual packages infected, but the trust-based build/release pipeline is also repurposed as a distribution vector. Also noteworthy is the reported collaboration between Team PCP (the cybercrime group central to this activity in Q1) and the newer RaaS collective Vect.

- The revelation of two phone exploit kits — Coruna and DarkSword — which were exploited as zero-day vulnerabilities for months not only by state-sponsored groups from Russia but also by Chinese crypto-criminals, points to an increasing proliferation of zero-days as "second-hand" goods, presumably sold by central brokers to various end customers.
- The conflict between the US, Israel, and Iran revealed further connections between criminal and state-affiliated actors, such as between Handala (aka Void Manticore) and the Radamanthys infostealer. Furthermore, North Korean APTs have been operating as affiliates of criminal "as-a-service" models — in this case, the Medusa ransomware gang. This creates new business opportunities for criminals, while state actors save on the costs of initial access.
- Other insights were discovered through OPSEC errors: for example, a North Korean actor infected their own system with the LummaC2 infostealer, which made it possible to confirm their involvement in the Polyfill.io supply chain attack. In another case, the INC ransomware group facilitated the recovery of stolen data from 12 organisations by repeatedly using the same backup infrastructure.
- In Q1, the ClickFix technique also established itself as a now-ubiquitous social engineering technique, with new sub-variants continuing to emerge, such as the so-called "CrashFix" variant from the KongTuke group. This variant intentionally crashes the victim's browser and causes it to execute malicious commands as well as a previously undocumented Python RAT.
- AI continues to gain prominence in the ransomware landscape; according to IBM, the Hive0163 group used an AI-generated C2 framework, which is easier to implement and carries less risk than, for example, autonomous AI agents. However, the conclusion was that the use of AI primarily served to accelerate the attack phases, rather than representing a novel form of threat in and of itself.
- In another case of extensive data theft from Mexico which affected nine government agencies, attackers used Anthropic's Claude Code and OpenAI's GPT-4.1 to drastically shorten the attack timeline, as well as to transform raw data from the reconnaissance of hundreds of servers into structured and usable information.
- As was the case in 2025, affiliates of particularly active RaaS groups (e.g., Qilin and SafePay) continued to focus heavily on small and medium-sized enterprises in Germany during Q1 2026, especially in the manufacturing sector. Here, too, AI plays an increasingly important role in overcoming language barriers.
- On a technical level, ransomware actors are also increasingly integrating EDR killers into their operations to disable security mechanisms just before encrypting data. In doing so, criminals are increasingly relying on the "Bring your own vulnerable driver" technique to extend their access privileges to the necessary system level (kernel).
- Law enforcement agencies and their partners also remained very active in Q1: Several takedowns occurred, such as the FBI's shutdown of the Russian-language underground forum RAMP, as well as the temporary shutdown of the infrastructure of the phishing-as-

a-service provider Tycoon2FA, which, however, resumed its activities after a short time. In addition, Google, together with other partners, took action against IPIDEA, the world's largest residential proxy network, whose services allow cybercriminals and state-sponsored APTs to conceal their identities.

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

Kerstin Zettl-Schabath is a Senior Cyber Threat Intelligence Analyst at the German Cyber Security Organisation (DCSO).

Jonas Hemmelskamp is the Chief Data Scientist at the European Repository of Cyber Incidents and is a doctoral candidate at the Institute for Political Science in the University of Heidelberg.

Lena Rottinger is a master's graduate of the University of Heidelberg and is an academic researcher with EuRepoC; she is responsible for the political coding of cyber incidents.

Erik Kellenter is a student assistant at the German Institute for International and Security Affairs (SWP) and is pursuing his BA in Political Science and MS in Computer Science.

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu