European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

Q2 2026

Kerstin Zettl-Schabath
Lena Rottinger
Erik Kellenter
Callahan Shelley

Overall observations

In the second quarter of 2026 (Q2), **162 new cyber operations** were added to the database: a 14% decrease compared to the previous quarter. The number of operations has thus continued to decline following a peak in activity in mid-2025; it is currently 9% below the long-term quarterly average. Overall, Q2 was heavily influenced by cyber operations carried out in the context of the conflict between Iran, the US, Israel, and the Gulf States.

With **51 incidents,** the United States remains the most frequently targeted country, accounting for nearly one-third of all recorded incidents. The ongoing conflict with Iran has been accompanied by an increase in attacks on US critical infrastructure. Meanwhile, at 37 incidents, the number of attacks against EU Member States declined significantly, falling by 18% compared to the previous quarter. Germany and France were the most frequently targeted EU Member States, with 11 incidents each, followed by Spain with 4 incidents; together, these countries accounted for two-thirds of all attacks on EU members.

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)**.

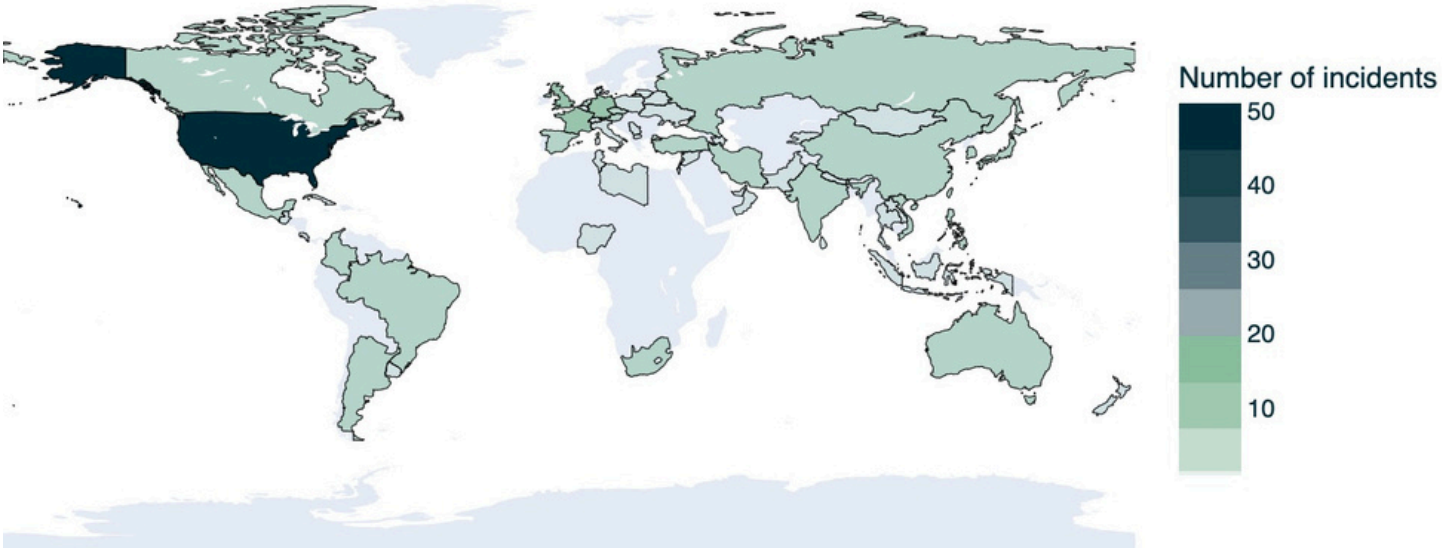
As of October 2025, EuRepoC prepares the Briefing on a quarterly basis in collaboration with the **German Cybersecurity Organisation (DCSO).** The German edition is published in partnership with the **Tagesspiegel Cybersecurity Background,** accessible here.

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 Q2 2026



In mid-April, threat actors targeted an external medical service provider in Germany, resulting in the theft of personal data belonging to approximately 61,000 patients from hospitals across the country. A trend of French government agencies falling victim to attacks continued: cybercriminals gained access to "Tchap," a messaging service used by the French government, via a compromised account linked to the Ministry of Education; the attackers then stole 643,459 messages from 73,467 individuals, including messages from several ministries. The United Kingdom tied with Germany and France, with 11 attacks.

Focal points and targeting patterns

The relative distribution of operation types remained consistent compared to the previous quarter. The largest share of incidents (84%) included "Hijacking with Misuse;" this classification is coded when an initial intrusion involves further malicious actions. In most cases, this means data theft or disruptions to IT systems, but the consequences of such activities can vary widely.

In late May, an unknown attacker manipulated Meta's AI support chatbot to gain access to the Instagram accounts of well-known figures, including the account of a Chief Master Sergeant in the US Space Force and an inactive account belonging to former US President Barack Obama, through which anti-American content was subsequently published.

The most common consequence of cyber incidents is data theft, which was reported in 62% of the incidents recorded. Nearly one-third of data theft incidents resulted in the data being leaked.

The most common cause of data theft is ransomware, which was used in 26% of the incidents recorded. In Q2, the ShinyHunters ransomware group was once again behind serious security breaches. Particularly noteworthy are the attack on the US education platform Canvas in May 2026, which affected nearly 9,000 schools and universities worldwide, and the exploitation of the zero-day vulnerability CVE-2026-35273 in Oracle's PeopleSoft enterprise software.

Distribution of Operation Types

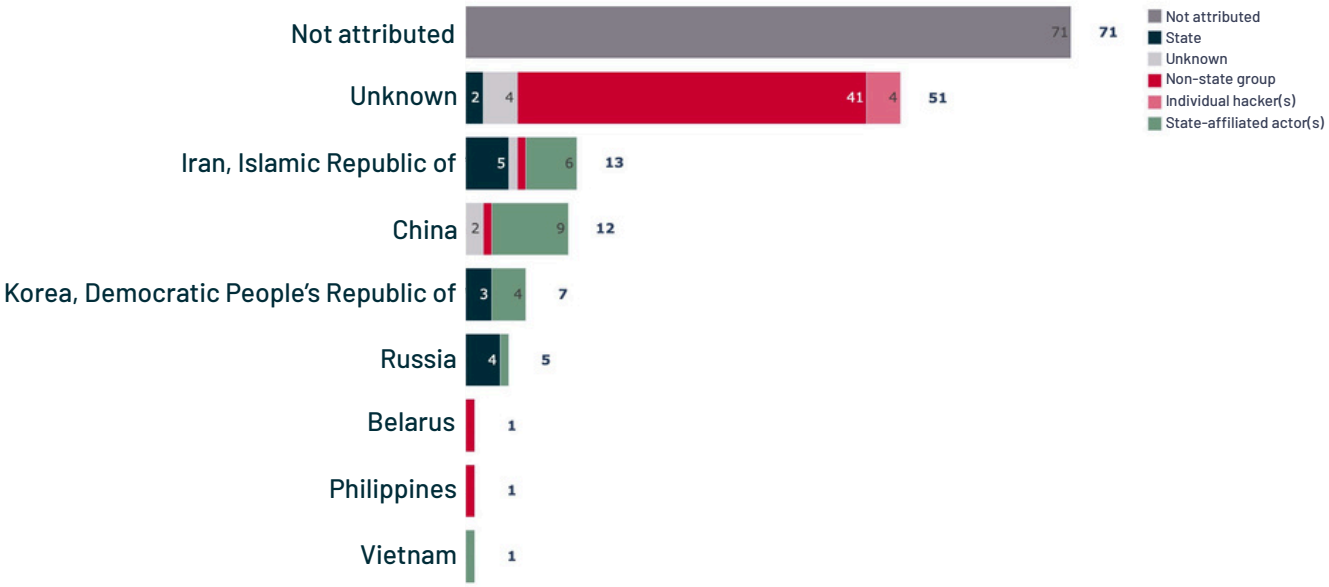
Note: Individual cyber incidents may have several operation types in combination

According to Mandiant and the Google Threat Intelligence Group (GTIG), the zero-day was used to attack over 100 organisations worldwide, including the University of Nottingham and other institutions. The use of zero-day vulnerabilities by ransomware groups is a new development; furthermore, the proportion of incidents in which at least one zero-day vulnerability played a role has doubled from 1.6% in the last quarter to 3% in Q2.

Disruption is the third most common type of attack (36%). In most cases, disruption follows hijacking (i.e., hijacking with misuse); however, disruption can also result from a DDoS (Distributed Denial of Service) attack. Compared to the previous quarter, the number of DDoS attacks has declined. Specifically, the share of DDoS attacks fell from 7% to 1% (compared to Q1 2026), while EuRepoC did not record any incidents involving the notorious Russian hacktivist group NoName057(16) in Q2, following several international law enforcement actions over the past 12 months.

“Hijacking without Misuse” accounted for 10% of the recorded incidents; these are incidents in which the attackers were stopped before serious damage could occur, or in which the impact on the victims remained unclear. This is typical of long-running espionage campaigns that are uncovered, for example, through telemetry data.

Suspected countries of origin of initiators in Q2 2026



Threat actor profiles and attributions

So far, approximately 56% of publicly reported cyber incidents recorded in Q2 have been attributed, with the CRINK countries (China, Russia, Iran, and North Korea) once again topping the list of attacking nations. While Russia and China typically accounted for the most attributions in previous quarters, Iran leads the list for the first time, with thirteen incidents.

More than half of the documented cyber incidents originating from the Iranian government are attributed to Handala Hack. As the name "Handala" suggests, the group operates under an ideological framing of resistance, primarily aiming to spread anti-Western and anti-Israeli messages. In this context, Handala compromised, for example, the National Center for Support of Holocaust Victims in Israel and "Iran Wire," a media outlet for exiled Iranians. Handala often claims responsibility during or after the attacks by disseminating information about the attack and stolen data via Telegram. Not all of these claims of responsibility can be verified, and EuRepoC documents only those cases where a CIA triad violation has been proven. However, even unverified claims of responsibility for an attack can cause reputational damage to the victims and sustain the psychological impact of the alleged disruption and destruction. In June, for example, Handala breached the networks of a California-based water utility (Cal Water), stole sensitive customer data, and subsequently published it. Handala also stated that it was capable of disrupting access to the water supply but had decided against doing so for the time being. Cybersecurity experts, however, were unable to find any evidence of a successful intrusion into operational technology (OT), but pointed out that Handala had successfully used custom-built wiper malware in previous attacks, which largely paralysed the victims' networks (see Handala's breach of Stryker).

In addition to Handala, other Iranian actors also targeted critical infrastructure. In light of the ongoing conflict between the US, Israel, Iran, and Gulf States, US authorities issued multiple warnings over the past quarter about Iranian attacks designed to exploit vulnerabilities in internet-accessible operational technologies (OT) and to digitally manipulate automatic tank gauge

systems (ATG). The latter activity has not yet been officially attributed by the US government, but media reporting links it to the Iranian government.

In addition to Iranian threat actors, Chinese actors were also particularly active in Q2. Two attributions stand out in particular: first, a report from the Five Eyes intelligence agencies regarding the targeted use of social networking sites and online job platforms to gather information, and second, Google's technical attribution revealing how the (allegedly) Chinese group UNC5221 exploited zero-day vulnerabilities. Overall, these cases demonstrate the well-known Chinese attack pattern of using cyber operations to steal valuable information from government agencies and private companies.

In early April 2026, a British advisory revealed that the Russian threat group APT28 was exploiting vulnerable routers to carry out DNS hijacking operations. Since 2024, APT28 had been redirecting its victims' traffic to DNS servers under its control, allowing it to harvest passwords, OAuth tokens, and other credentials for web and email services. In this context, US authorities also took operational action to shut down the US portion of the compromised router network. APT28, also known as Forest Blizzard, Fancy Bear, and STRONTIUM, is attributed to the Russian military intelligence service (GRU) and is one of the most active Russian threat actors.

In April, German media also reported that the Signal accounts of high-ranking German politicians had been successfully compromised. Those affected apparently included Bundestag President Julia Klöckner (CDU), Education Minister Karin Prien (CDU), and the Minister for Housing, Urban Development and Building, Verena Hubertz (SPD). As early as February, the BSI and the BfV warned of phishing attacks via the messaging services Signal and WhatsApp and suspected that state-sponsored actors were behind them. While Dutch intelligence agencies explicitly named Russia as the responsible state, the German federal government has not yet officially attributed the incident.

Developments in the cybercrime ecosystem

Key observations from Q2 can be summarised as follows:

- The relationships and division of roles within Ransomware-as-a-Service (RaaS) structures are becoming increasingly flexible and complex. For example, the "FortiBleed" campaign has been linked, through a shared affiliate, to the Lynx and INC Ransom groups, which also regularly target German companies. The central role of "TOXMAN" in technical development, execution, and ransom negotiations also suggests that individual affiliates are taking on a broader range of responsibilities. While this allows RaaS groups to offload risks to these affiliates, it also creates new opportunities for detection and attribution due to operational overlaps.
- Another indication of the growing flexibility of the cybercrime ecosystem is a Microsoft report on the "Malware-signing-as-a-Service" (MSaaS) actor "Fox Tempest:" this actor offers criminals, such as ransomware groups, short-term, seemingly legitimate software certificates, allowing their malicious code to bypass security processes.
- Meanwhile, it is becoming increasingly common for multiple actors to compromise the same target. Whether coordinated, intentional, or completely independent of one another, such multiple compromises complicate ongoing defense efforts, as well as the

forensic and damage assessment processes that take place in the aftermath of an incident.

- The link established between Chaos ransomware operations and the Iranian APT MuddyWater once again underscored the fact that what appear to be criminal ransomware attacks may in reality be the work of state-affiliated actors.
- The current most active RaaS group is "The Gentlemen." It develops and operates its own EDR-killer suite, which is made available to its affiliates. Unlike older RaaS groups such as Qilin or Akira, however, its target profile is more international and less focussed on the US. What they have in common, however, are the numerous attacks against German companies. In Q2 as in previous quarters, ransomware and extortion posed a significant risk in Germany, originating from both established RaaS actors and "newcomers" such as Settra and Krybit.
- In recent months, Chinese cybercriminals such as TA4922 — who most recently targeted victims in Germany, Italy, the United Kingdom, and South Africa — have also shown similar "globalisation trends." These operations, which are aimed at fraud through data theft and the sale of login credentials, primarily incorporate seasonal topics related to HR, taxes, and payroll processing into their social engineering tactics.
- At the tactical level, ClickFix, along with its constantly-evolving subvariants, remains the tool of choice for many leading initial access brokers. Specifically, KongTuke, for example, used this technique to plant a previously unknown backdoor called Mistic on opportunistically selected target systems, which led, among other things, to compromises by Qilin affiliates.
- Open-source supply chains also remain a target for many cybercriminals, for example, to spread infostealers. Specifically, in one case, the attackers targeted Claude and Gemini users, thereby combining two particularly prevalent attack vectors.
- In general, criminal (as well as state-sponsored) attackers are increasingly using AI workflows and applications as potential entry points into target systems. For example, in Q2, attackers exploited vulnerabilities in OpenClaw's "Skill" architecture, which allowed them to distribute a remote access Trojan. Unverified third-party plugins can thus grant attackers access to AI-powered systems.
- However, criminals, such as the extortion-focussed group FulcrumSec, have also diversified their own use of AI. For example, the group used AI agents to analyse stolen data more efficiently.
- As an example of the numerous law enforcement actions taken in Q2, the international "Operation Endgame" achieved further successes, this time against the malware SocGholish, as well as Amadey and StealC. In the case of SocGholish, 106 servers and domains were taken down, and approximately 15,000 compromised WordPress sites were cleaned up. The debate over the legal basis for such actions is likely to continue, particularly in the broader context of the ongoing legislative proceedings in the field of security in Germany.

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).

Lena Rottinger is a doctoral candidate the University of Heidelberg and is an academic researcher with EuRepoC; she is responsible for the political coding of cyber incidents.

Callahan Shelley is a researcher at the German Institute for International and Security Affairs (SWP) within the Research Division EU/Europe.

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