European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

Q3 2026

Kerstin Zettl-Schabath
Lena Rottinger
Callahan Shelley
Erik Kellenter



Overall observations

In Q3 2026, **227 publicly disclosed cyber operations** were added to the EuRepoC database. This represents a substantial increase (40.1%) compared to the previous quarter and 36 more operations than the overall average of 191 cyber operations per quarter recorded over the entire period between 2000 and 2026.

With **64 incidents, the United States remains the most frequently targeted country**. EU Member States were affected in 67 incidents: France was the most frequent target, with 25 incidents in Q3 (compared to 11 incidents in Q2); this was followed by Germany (11) and Spain (8).

Particularly noteworthy is the "ShinyHunters" attack on the US Federal Bureau of Investigation (FBI), in which more than 3 TB of data on FBI employees was stolen. At the same time, ShinyHunters demanded that a report on the group be withdrawn. Shortly thereafter, a coordinated operation by US and international authorities led to the arrest of several suspects. Meanwhile, the military conflict surrounding Iran

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)**.

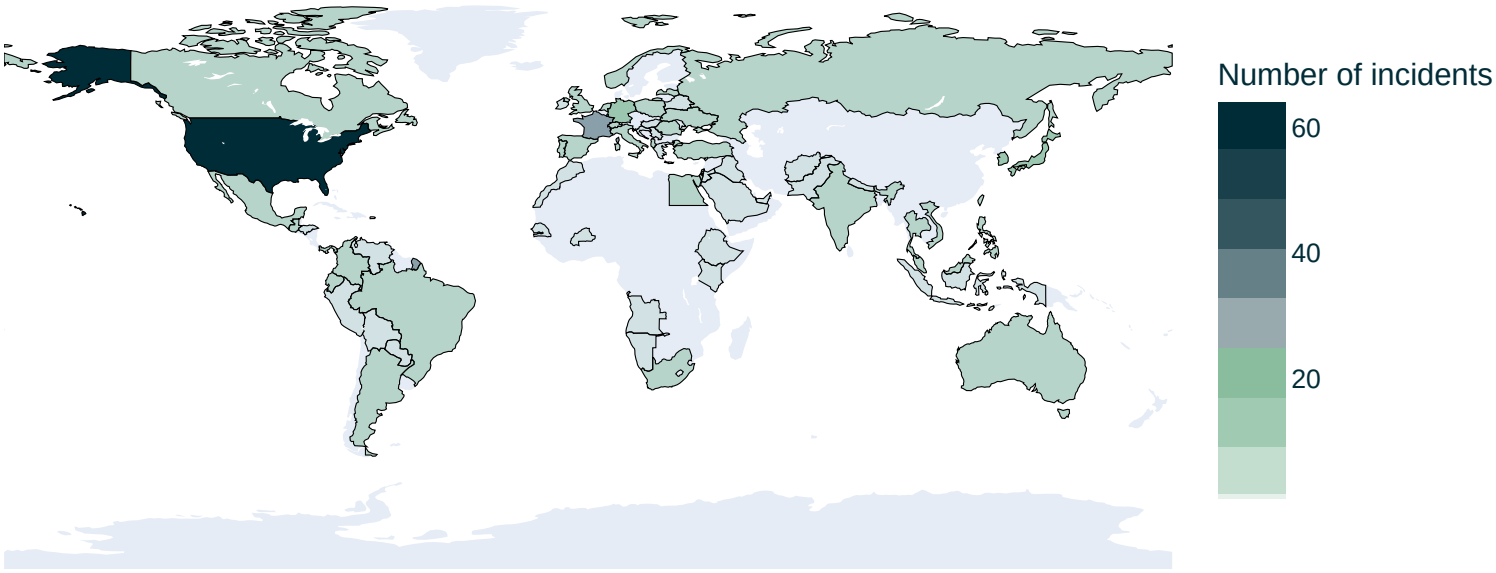
As of October 2025, EuRepoC prepares the Briefing on a quarterly basis in collaboration with the **Deutsche CyberSicherheitsorganisation GmbH (DCSO).** The German edition is published in partnership with the **Tagesspiegel Cybersecurity Background,** accessible here.

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 Q3 2026



continued to play a significant role in the US cyber ecosystem as well; several incidents were recorded that targeted water supply systems in multiple states, including New Jersey and Minnesota.

In France, attacks were carried out in August against the Ministry of Housing and Urban Development and the Ministry of Ecological Transition. In late July, unknown actors also breached the Ministry of Education, resulting in the theft of personal data belonging to ministry employees. In Germany, in addition to the theft of information from the Berlin Senate by the ransomware group "Rhysida," organisations in the telecommunications, healthcare, energy, research, and transportation sectors were attacked, while in Spain, the healthcare, research, and transportation sectors were affected.

Focal Points and Targeting Patterns

The relative distribution of attack types has remained largely consistent compared to the previous quarter. The majority of the cyberattacks recorded (86%) fall under the category "Hijacking with Misuse." This means that an attacker not only gained access to IT systems, but also caused damage — most often by stealing and/or encrypting confidential data and/or crippling systems. Just under one-third of these recorded cyberattacks were ransomware attacks. The proportion of incidents involving data theft ("Data Theft") totaled 60% this quarter, with the stolen data being published in 17% of cases ("Data Theft & Doxing").

In 42% of the incidents recorded, the cyberattack resulted in a disruption of the victim's systems, an increase of 6% compared to the previous quarter and the highest figure since early 2025. In most cases, system outages are a consequence of a successful compromise. Only in 6% of

Distribution of Operation Types



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

cases was the disruption caused by a DDoS attack — a significant decline, as DDoS attacks accounted for 20% of incidents in the same quarter last year.

In this quarter, there was a particularly severe attack on the Romanian Land Registry Authority (ANCPI), during which sensitive data was stolen and the country's entire land registry database was allegedly deleted. Although reports indicate that the database was later restored from a backup, all real estate transactions were blocked for several days, preventing notaries from certifying sales and citizens from obtaining land registry extracts.

Threat Actor Profiles and Attributions

In Q3, more than half of the publicly reported cyber incidents (53%) were not attributed. As in previous quarters, Russia, China, Iran, and North Korea top the list of attributed states. Unlike in Q2, however, Russia — not Iran — accounts for the most incident attributions, with several cyberattacks attributed to Centre 16 of the Russian Federal Security Service (FSB).

According to a joint official attribution by the United Kingdom and the EU on 13 July 2026, Centre 16 is responsible not only for the attack on the Polish energy sector in late December 2025, but also for a series of other attacks on EU Member States such as

France, Germany, Cyprus, the Netherlands, Austria, Slovakia, Romania, and Finland, as well as EU partner states (in particular Ukraine). Centre 16 has been active since at least 2010 and primarily targets government institutions and various critical infrastructure sectors, including energy, aviation, water, and industrial manufacturing. This is the first EU statement in which Centre 16 has been explicitly named as a threat actor. What is notable about the European response is the extent of coordination and information sharing, the accompanying measures, and the apparent absence of the US as a leading actor.

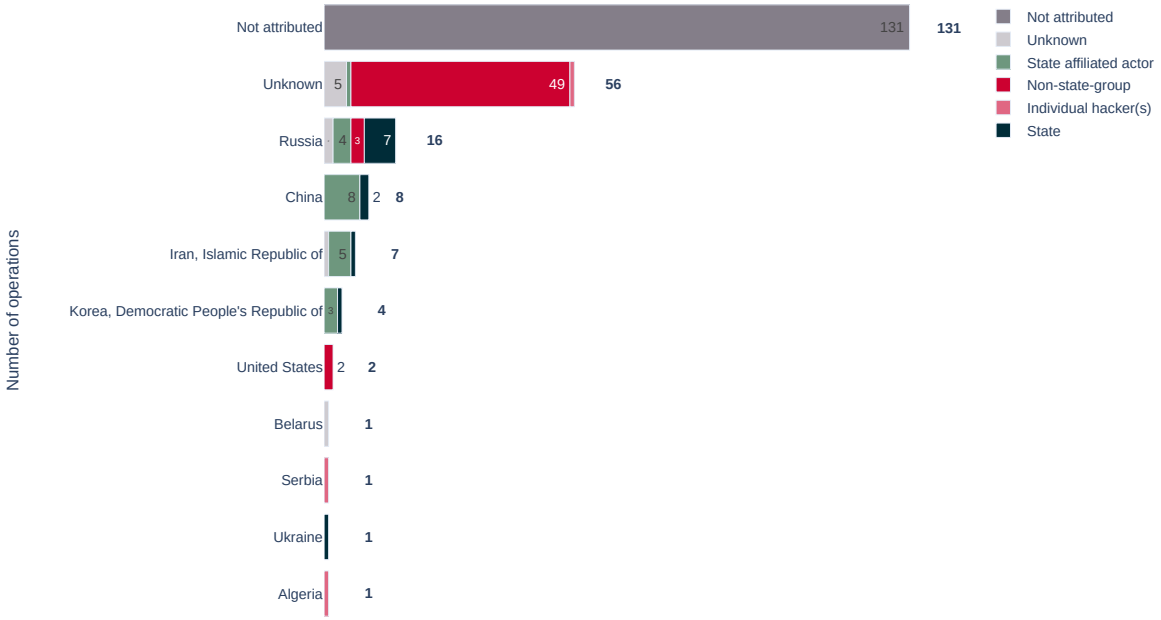
In addition to the EU statement and the British attribution, Germany, France, and Poland issued separate statements that are noticeably different in terms of their specifics and tone. In a separate statement, France revealed that TURLA (a subgroup of Centre 16) had attacked the Ministry of the Armed Forces in 2017, the French Embassy in Moscow in 2018, the justice sector in 2019, and a research institution specializing in sensitive technologies in 2026. None of these incidents had previously been documented in the EuRepoC database, meaning they have now been made public for the first time. This marks France's second official political attribution of Russian state-sponsored cyber activities and could signal a new, more assertive French cyber attribution policy.

The accompanying German and Polish press statements, on the other hand, were significantly more restrained and provided no new information about the cyber activities of Centre 16. These statements merely confirmed that the group successfully compromised facilities in both countries, but no further details were disclosed (not even upon request at the Federal Press Conference).
This array of responses, which was supplemented by the summoning of Russian ambassadors in several European countries, a British-European package of cyber sanctions, and a joint advisory on router security, points to a Europeanisation of international cyber diplomacy. Until the second Trump administration, such Western responses were strongly shaped by US initiative. Overall, this coordinated set of responses sends a clear signal that joint action, even without US leadership, is possible.

AI and Attacker Profiles

Artificial intelligence (AI) continues to gain importance both as a tool for attackers and as a target of attacks. In Q3, there was an increasing integration of AI into attack cycles, as well as the emergence of a new type of attacker: autonomous AI agents (see the Hugging Face incident). Two trends are particularly noteworthy here: first, less professional and less well-resourced actors are increasingly able to carry out more complex cyberattacks, as AI models can work faster, more efficiently, and on a larger scale than humans when it comes to target selection, vulnerability identification, and penetration of external networks. In addition, stolen API keys were used to tap into additional AI computing capacity during the course of the attack. The use of AI agents is demonstrably being driven by Russian (e.g., Midnight Blizzard), Chinese, Iranian, and North Korean actors with ties to their respective states. Second, the degree of autonomy of these AIs is steadily increasing, meaning that cyber operations are increasingly AI-led rather than "merely" AI-assisted. However, initial claims regarding fully autonomous (ransomware) attacks must be viewed with caution. For example, the company that reported on the allegedly fully autonomous AI agent JADEPUFFER

Suspected countries of origin of initiators in Q3 2026



subsequently had to admit that it did not operate as autonomously as had initially been portrayed in relation to its ransomware activities.

Developments in the Cybercrime Ecosystem

In Q3, the following developments in the area of cybercrime were particularly noteworthy:

New groups such as Gammax and Orova increasingly relied on "double extortion," in which data is first exfiltrated and then systems are encrypted. Stolen information is increasingly being monetised multiple times, for example by extorting affected customers of the primary victim. At the same time, the lines between financially-motivated cybercrime and state-sponsored activities remain blurred. The observed overlaps between the ransomware group Gunra and Lazarus illustrate this trend but do not automatically prove that individual operations are state-sponsored. Flexible networks of actors, regional sub-structures, and shifting collaborations continue to complicate attribution. Arrests of suspected members of ShinyHunters and TeamPCP also show that, while law enforcement measures are having an impact, the underlying networks remain persistent and complex.

At the tactical level, device-code phishing remained a significant initial access vector. Commercial phishing-as-a-service offerings such as Greatness, DEBULL, and ARToken enable scalable attacks and increasingly combine Microsoft authentication methods with adversary-in-the-middle techniques. Since these attacks do not require traditional fake login pages, they can be more difficult for employees to detect. In addition, vishing combined with mail-bombing gained prominence, particularly as a means of gaining initial access. The DCSO observed this technique in several incident response (IR) operations in Q3: attackers first flood their victims' inboxes and then pose as IT support over the phone to gain access to corporate systems via legitimate remote maintenance tools. Fake recruiting requests and advanced ClickFix techniques further expand the spectrum of attacks. In ClickFix attacks, victims are tricked into entering commands directly into the browser's address bar; such attack chains often lead to the installation of information

stealers such as Amatera and Remus. Overall, social engineering and the deployment of attack tools are becoming increasingly sophisticated and are being adapted to existing defensive measures.

Meanwhile, the CRPx0 group, which operates under a white-label ransomware-as-a-service model and promotes its services very publicly, including via YouTube and Spotify, proved that — contrary to the prevailing pattern — criminals can focus on crypto scams even at the start of their "careers" and only begin carrying out ransomware operations over time. Paying ransom to such actors is not a recommended response: according to Proofpoint, in 2026, an average of 37% of recorded ransomware victims worldwide were extorted again despite having paid the ransom. In addition to executives, employees in finance, human resources, and sales are specifically targeted by criminals. Software developers and software ecosystems such as npm also remain relevant targets, especially for supply-chain attacks such as the self-propagating "ChainDrop" operation.

Several incidents also highlighted the potential impact on critical business operations and public institutions: a ransomware attack on the Health Sciences Centre in Winnipeg disrupted not only other building systems but also door locks, as well as heating and air conditioning systems. Ernst & Young reported a data breach that could also expose its clients to potential blackmail. In Liechtenstein, approximately 31,000 data records were stolen from a register of beneficial owners, which is particularly sensitive in the context of combatting money laundering and the financing of terrorism.

Particularly serious was the leak of 5.8 TB of confidential data following the aforementioned attack by the Rhysida group on the Berlin Senate. In addition, previously undisclosed vulnerabilities in SonicWall SMA-1000 systems were exploited by ransomware attackers. The shortened time frames between initial access and data disclosure by the initial access broker make it difficult in such cases to contain compromises that have already occurred through retroactive patching alone. This was presumably also the case for three Citrix NetScaler vulnerabilities that were exploited as zero-day exploits starting in late September.

Internationally, there were the aforementioned arrests of suspected members of ShinyHunters and TeamPCP, as well as actions taken against suspected members of Russian hacktivist groups and Scattered Spider. At the same time, the new US presidential directive dated 12 August authorising private contractors to combat "cyber-enabled transnational crime" raises questions about associated risks. The same applies to the increased cooperation between the US, China, and Russia in handling sensitive information — as announced by FBI Director Kash Patel — and the associated security risks.

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 at 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