European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

January 2024

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

Overall observations

In **January 2024**, EuRepoC recorded 86 cyber operations, marking a 41% surge from the previous month and surpassing the overall average in recorded activity of 64 cyber operations per month by 22.

The **average intensity** of operations recorded in January 2024 registered at 3.4, exceeding the historical average (2.8). The notable uptick in operations since February 2023 is partly attributed to an expansion in EuRepoC's 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 January, but may have started earlier. The focus is on technical, political, and legal aspects.

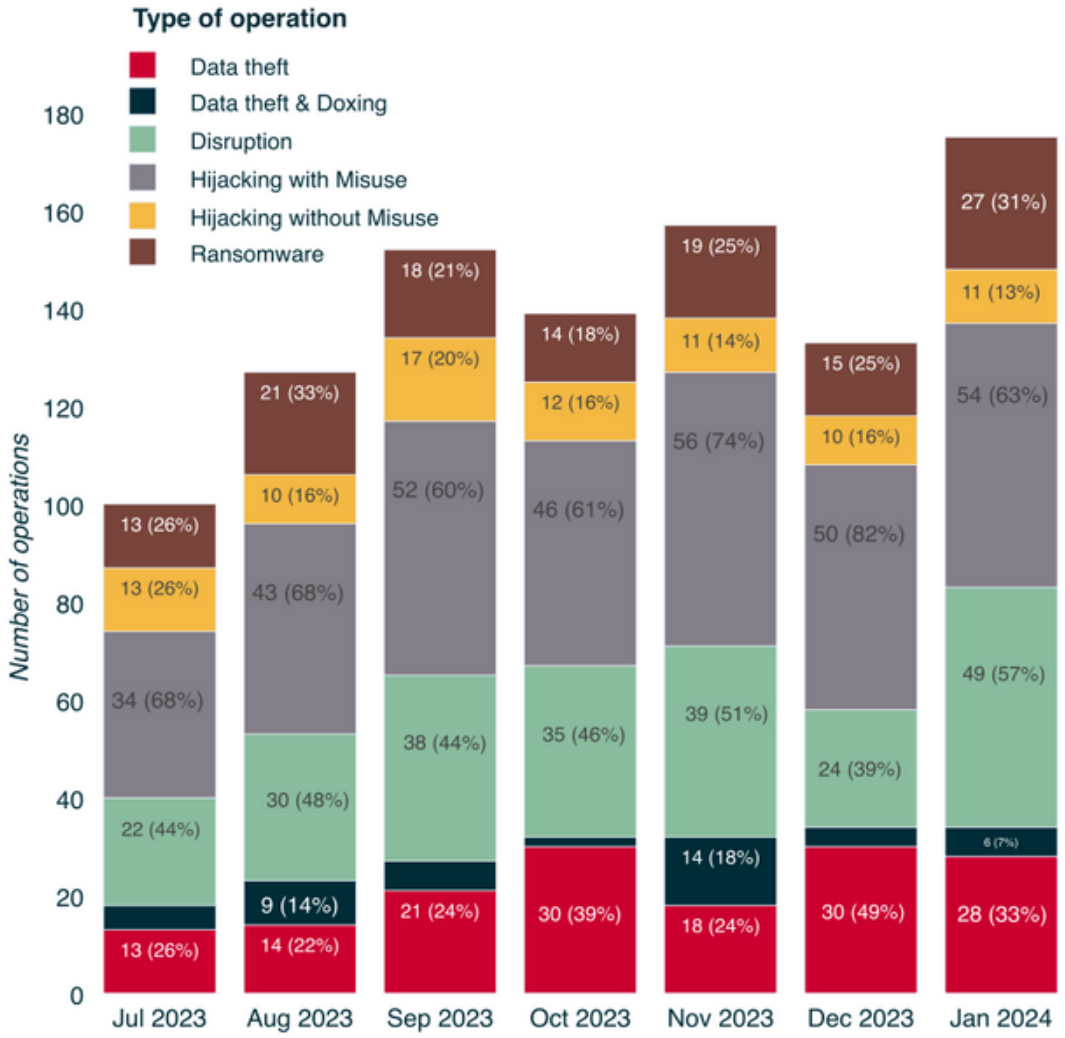
About EuRepoC

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 January 2024 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 of activity tracked in January comprises **"hijacking with misuse"** operations, with 54 cases (63%). As an umbrella term, this describes operations in which threat actors have succeeded in penetrating systems and networks to carry out unauthorised, harmful actions. Where collection on these indicators is possible, EuRepoC differentiates these activities further by threat actor intent and, if applicable, identifies data theft or operational disruptions.

The second most common type of operation identified in January was "disruption" operations (57%). This refers to operations with the aim of disabling an information technology service. In this regard, a disruption or interference impairs its availability. Disruption operations are usually temporary in nature. In the case of ransomware, however, blocked access to critical data can also cause downtime over a longer period of time. EuRepoC recorded 49 of these operations in January.

A particularly attractive target for "hijacking with misuse" operations is hardware that manages data traffic at gateway points between two networks and, for example, connects companies and government organisations to the public Internet through encrypted channels.

Such edge devices are often difficult to secure with conventional security solutions. Several Chinese espionage groups with suspected state connections have been observed to specialise in finding previously unknown vulnerabilities in these devices and exploiting them as entry vectors. The effort involved in discovering these vulnerabilities initially limits this possibility to actors who have access to substantial resources, in particular state-sponsored groups. However, the frequent use and disclosure of these vulnerabilities currently observed point to a growing risk that these capabilities will spread to a wider range of threat actors through proof-of-concept exploits (PoCs). Unlike state-sponsored espionage units, financially-motivated actors or hacktivist groups may not apply the same care in narrowly selecting their targets. The disclosure of zero days as a result of state-sponsored operations therefore has the potential to extend the exploitation of these vulnerabilities to a broader attack surface of vulnerable edge devices, as less discriminating actors adapt these capabilities. A documented example of these risks is the multi-stage espionage campaign against edge devices manufactured by Ivanti, which was reported in January.

On 10 January, Ivanti reported two newly discovered vulnerabilities (CVE-2024-21887 and CVE-2023-46805) in two of its VPN solutions - the Ivanti Connect Secure and Ivanti Policy Secure gateways. As confirmed by threat intelligence companies Volexity and Mandiant in coordination with Ivanti, at least one Chinese espionage group has been using the vulnerabilities in Ivanti Connect Secure since 3 December 2023 to gain access to vulnerable edge devices.

When chained together, the vulnerabilities make it possible to remotely execute arbitrary commands on the target systems. Through this vector, the actor tracked by Mandiant and Volexity as UNC5221 and UTA0178, respectively, was able to obtain additional credentials and to expand its access in the target environment.

Prior to the publication of its findings on 10 January, Volexity only had evidence of one organisation being compromised through the two detected zero days. This initial narrow scope suggests careful targeting by UTA0178/UNC5221 in an attempt to evade early detection.

Shortly after this disclosure and provision of mitigation measures, UTA0178/UNC5221 changed its approach on 11 January, opting for widespread exploitation of unpatched systems. On 15 January, just days after the vulnerabilities were disclosed, infections with the GIFTEDVISITOR webshell, a tool used by UTA0178/UNC5221 to send commands to compromised devices, indicated more than 1,700 affected systems worldwide. A day later, this number stood at 2,100, with a range of targets in the telecommunications, financial, technology, defence, and aerospace sectors. This shift away from the group's initial narrow targeting shows signs of opportunistic exploitation as the window of opportunity started to close.

Supported by vulnerability scanners, publicly available blueprints to exploit vulnerabilities, and automated ways to customise attack tools, a number of actors with no known connection to UTA0178/UNC5221 were observed utilising the vulnerabilities for their own purposes.

For instance, the deployment of cryptocurrency miners via unpatched vulnerabilities indicates diverging intentions in a growing field of actors.

In contrast, UTA0178 had prized operational security, introducing modifications to Ivanti's built-in Integrity Checker Tool to subvert detection.

On 31 January, Ivanti announced two more zero-day vulnerabilities in its VPN appliances (CVE-2024-21888 and CVE-2024-21893). Mandiant confirmed the exploitation of the vulnerabilities by known Chinese espionage actors. The group, known as UNC5325, specifically exploited one of these newly discovered software vulnerabilities (CVE-2024-21893) to subvert mitigations released by Ivanti on 10 January.

A fifth zero-day reported by watchTowr on 2 February and disclosed by Ivanti on 8 February (CVE-2024-22024) was discovered before exploitation in the wild.

The widespread exploitation of the Ivanti vulnerabilities by independent actor clusters within a short period of time after disclosure indicates a proliferation risk posed by the vulnerability research of sophisticated espionage groups.

The rapid dissemination of vulnerability knowledge, facilitated by partly automated exploit development, enables newly-reported vulnerabilities to be operationalised as zero-days in unpatched target environments. This broadens the scope, particularly for actors who would not be able to develop this capability on their own.

Offensive security research labs, such as watchTowr, have recognised the responsibility involved in publishing weaponized PoCs. These PoCs accelerate the exploitation timelines of threat actors, particularly during time-sensitive periods when vulnerable organisations are still patching vulnerabilities. With respect to the vulnerabilities in the Ivanti gateways, watchTowr identified a direct correlation between the release of PoCs and efforts at mass exploitation.

The urgency resulting from this combination of critical vulnerabilities and expanding exploitation has prompted a turn to stopgap measures. On the day the second set of vulnerabilities became public, the US Cybersecurity and Infrastructure Security Agency (CISA) directed federal agencies to disconnect all Ivanti Connect Secure and Ivanti Policy Secure instances from their networks.

In the beginning of March, CISA confirmed the exploitation of two systems in its own networks earlier in February. An unnamed source identified the two systems as the Infrastructure Protection (IP) Gateway and the Chemical Security Assessment Tool (CSAT). Both systems hold sensitive information on critical industrial nodes and were taken offline upon detection of the compromise. IP Gateway contains information about connections between US infrastructure operators. CSAT archives security documents of companies in the chemical sector. Occurring after the public disclosure of the vulnerabilities and when initial mitigations were available, the intrusions affecting CISA underscore the challenges in remediating weaknesses faced even by mature organisations.

The increased use of zero-day exploits observed in the campaign against Ivanti devices is notable in two respects. Firstly, the fact that Chinese espionage groups are aiming to exploit two additional zero-day

vulnerabilities in the same products at high operational tempo, despite the heightened scrutiny following the discovery of the two initial vulnerabilities, suggests access to a purposefully developed repository of vulnerabilities. Secondly, the sustained efforts to continue the compromised operation indicate that the consequences of discovery, including a potential proliferation of capabilities, is of secondary importance in the strategic consideration of threat actors.

State-directed initiatives to stockpile vulnerabilities - supported by hacking competitions and legal requirements to centrally report vulnerabilities prior to disclosure - have drawn scrutiny over their role in perpetuating this combination of access to vulnerability knowledge and indifference to the impact of its proliferation.

Focal points and targeting patterns

In January 2024, critical infrastructure entities remained the most affected organisations, representing 53 new cases (62% of recorded cases). This continues the trend observed in previous months, where roughly three out of five incidents affected this sector. Compared to December, which saw 34 incidents, this marks a noticeable increase of around 55%.

State institutions were the second most affected targets, with 42 cases (49%), showing an increase of 18 cases (75% in relative terms) compared to the previous month.

The United States led the list of most frequently affected countries with 25 incidents, accounting for 29% of incidents, in line with the trends of the previous months.

EU member states were similarly affected, with a total of 24 incidents. France and Germany were the most affected member states, with six and four incidents respectively. Outside the EU, Canada ranked between the two countries with five incidents. The ongoing cyber dimension of the war against Ukraine is evident with four new incidents recorded on each side by Russia and Ukraine.

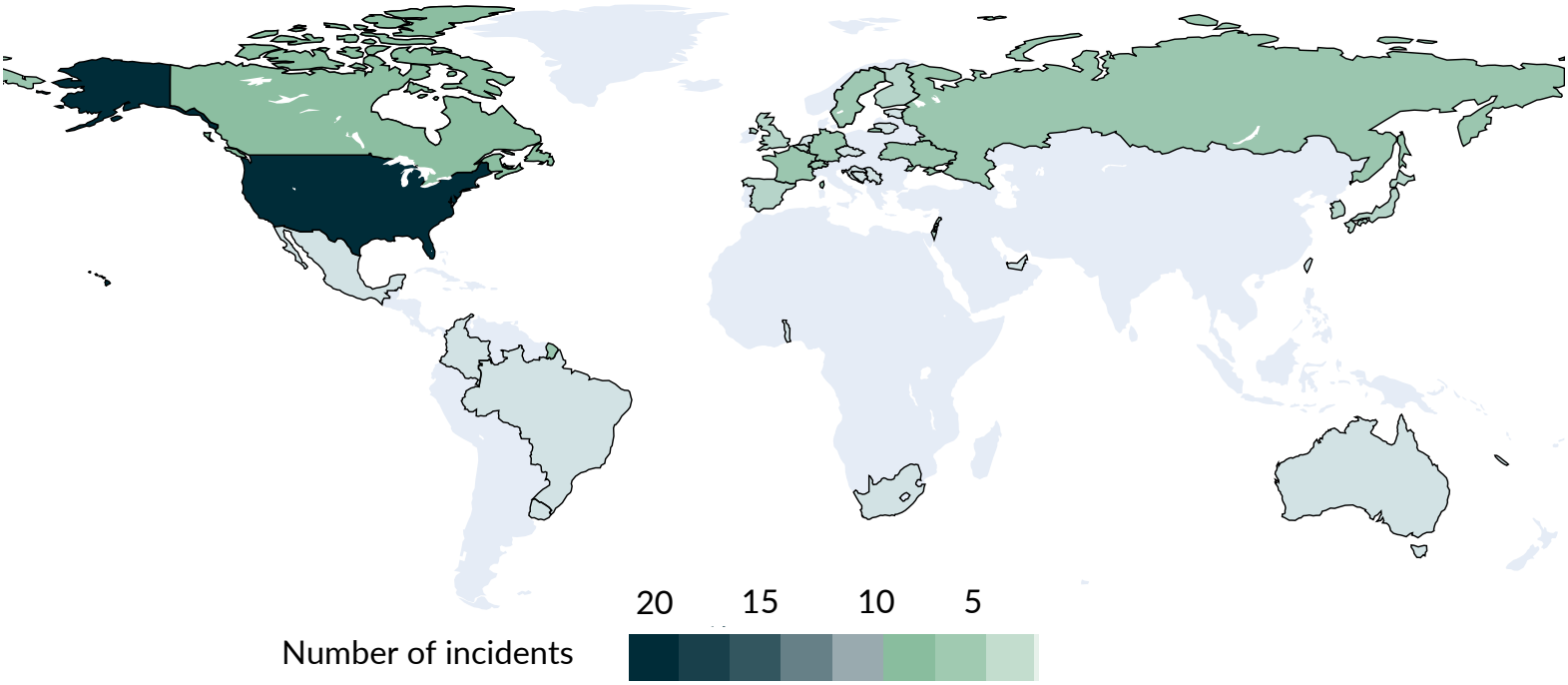
Among critical infrastructure targets, the financial and telecommunications sectors were the most affected in January, with nine incidents each. In the financial sector, this involved several thefts at cryptocurrency service providers such as Orbit Chain, Radiant Capital, and CoinsPad.

While the perpetrators of the Orbit Chain and Radiant Capital cases remain unknown, the North Korean threat actor Lazarus has been linked to the CoinsPad incident. The group was suspected of being behind an earlier attack against the platform in July 2023. In the crypto sector, Socket.Tech, a company specialising in the interoperability of blockchain networks, experienced a loss of crypto assets. Additionally, loanDepot, a financial company offering mortgage and non-mortgage lending products, was affected by a ransomware attack.

In the telecommunications sector and for digital providers, the types of cyber incidents observed in previous months persists. Several incidents indicate infiltrations by state or state-affiliated actors for espionage purposes, exemplified by a data theft at Hewlett-Packard in May 2023, which was disclosed in January 2024.

Moreover, a telecommunications service provider in New Caledonia suffered a compromise, alongside disruptive incidents targeting mobile and Internet providers such

Geographic distribution of operations



as Russian AKADO Telekom or Orange Spain. The sector remains a high-profile target of ransomware attacks.

The healthcare sector, alongside critical manufacturing, saw frequent incidents, with eight incidents recorded in January. The encryption and theft of data from networks at the healthcare centre Bezirkskliniken Mittelfranken was the only critical infrastructure incident which affected Germany.

For government institutions, there was a notable shift compared to previous months: 30 incidents affected subordinate administrative authorities, classified under "Civil Service/Administration." By comparison, ten incidents were directed against "Government/ministries" at the national level.

Operations against state institutions show a variegated picture. However, initial correlations emerge for the incidents recorded in January: twelve out of 13 ransomware attacks affected the civil service/administration sector, indicating a sustained pattern of opportunism with cybercriminals taking advantage of poorly secured systems.

Yet, incidents like those at the Serbian state energy supplier EPS, or the incident at the IT service provider Tietoevry which caused widespread system failures at Swedish universities and retailers, underscore the far-reaching consequences of ransomware. The latter incident in particular highlights the intertwined vulnerability of state entities and essential service providers when IT service providers in the supply chain are targeted.

Threat actor profiles and attributions

In January, the majority of cyber incidents recorded by EuRepoC remained initially unattributed, meaning that neither the type of attacker nor their country of origin/sponsor were named by the attribution sources recorded by EuRepoC. Nevertheless, the relative share of 57% is notably lower than in November, when it stood at 70%. For the remaining 43%, the attacker type (e.g., hacktivists, cyber criminals, state-sponsored proxies, etc.) was identified in 21 incidents, but not the suspected attacker country of origin or sponsor country. This is often the case for technical reports from threat intelligence companies addressing APT activity, which are typically suspected to operate at close direction of government agencies.

While some evidence points to potential countries of origin of the operations or their political clients, certain threat intelligence companies (such as Kaspersky) decide against directly attributing operations to specific state sponsors.

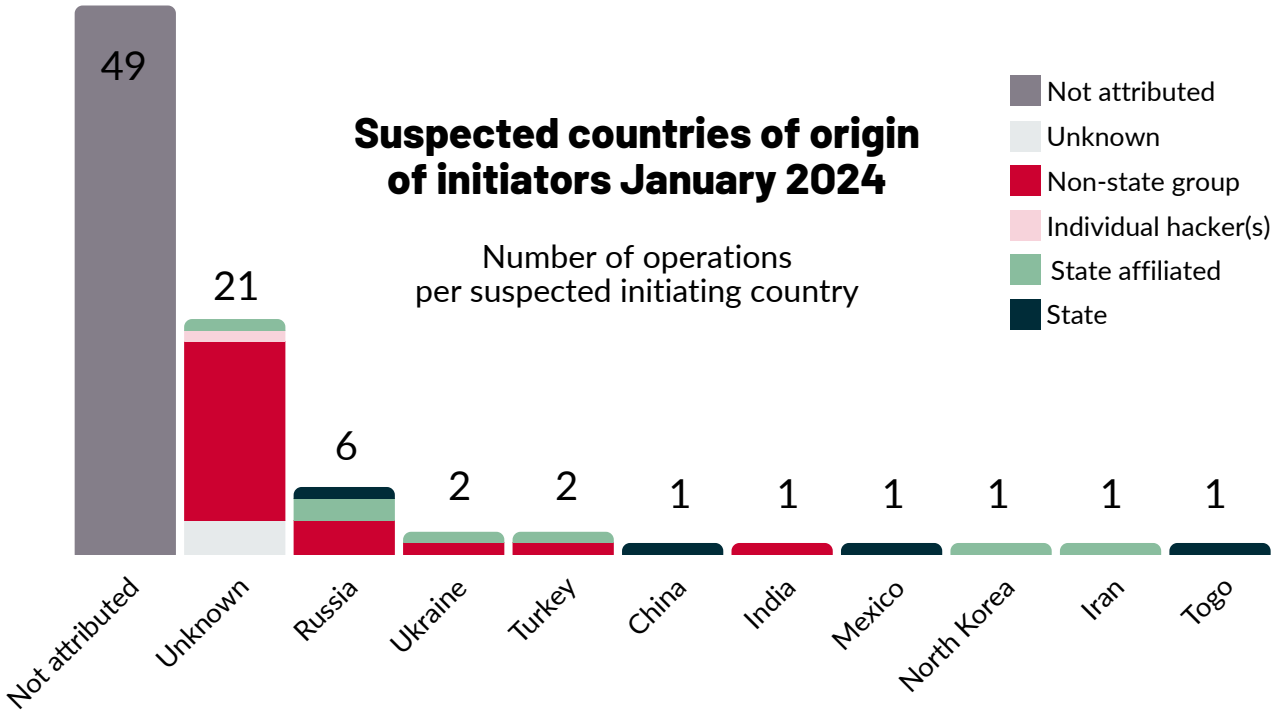
Non-state groups or individual hackers were accountable for 23 of January's 86 incidents. At 27% of the total, this is roughly 6% less than in November. Of these 23 operations, 15 were attributed to criminal actors, while six were attributed to politically/ideologically motivated hacktivists. One operation was linked to an individual hacker. The proportion of criminally motivated operations rose marginally compared to November, from 16% to 17%, while the proportion of hacktivist operations in total operations fell sharply: from 14% to just 7%.

With a total of 7 incidents (8%), the proportion of incidents attributed to proxies, i.e., groups supported or directed by states, remained almost the same as in November (7%).

Among criminally-motivated operations involving ransomware, nine different groups were responsible for the 15 recorded extortion attempts. Although new groups continue to emerge, a core of consistently active groups, such as LockBit, Medusa, Qilin, BlackCat/ALPHV, and the Cactus group, persisted over the last months. Whether or in which form LockBit will be able to reconstitute, following the disruption of its operations by law enforcement announced in February, remains to be seen.

Notably, the 15 ransomware operations targeted 14 different target sectors, encompassing various critical infrastructure operators and government entities.

Ransomware groups have increasingly shifted their focus to so-called "cyber big game hunting" in recent months, targeting critical entities expecting a higher probability of payment. However, recent analyses by the threat intelligence industry suggest a contrary trend, especially ransomware cases involving data theft, where victims have shown to be less likely to comply with ransom demands. At the same time, deliberations about government bans on ransomware payments raise questions about their effectiveness in reducing operations. An increase in unreported cases as a result of such restrictions - as operations continue unabated and paying victims refrain from reporting incidents to the authorities out of concern of retribution - is a distinct possibility. The impact of such payment bans on both attacker and victim behaviour remains uncertain.



The decline in hacktivist incidents compared to November is in part attributed to the lower level of activity recorded for Russian and Ukrainian hacktivist groups in January, which consistently accounted for the majority of hacktivist operations in previous months.

For example, only one operation by the group NoName057(16) was recorded on the Russian side in January. The same applies to the pro-Ukrainian IT Army of Ukraine. One operation each was attributed to Turkish and Indian hacktivists, countries that in the past have shown a high level of non-state, ideologically motivated cyber conflict activity due to their direct (India vs. Pakistan) and indirect (Turkey as a supporter of Azerbaijan in the conflict with Armenia over Nagorno-Karabakh) involvement in conventional conflicts.

January's list of attributed attacker countries of origin is characterised by a high degree of diversity, with numerous countries associated with one or two operations. Autocratic countries like China, Russia, Iran, and North Korea, though present, are less dominant this time.

Notably, a significant proportion of incidents are attributed to specific types of attackers without additional information about the countries of origin. Without a direct attribution to a specific country, this information still allows for assessments of intentions and capabilities and for raising awareness about targeted sectors.

In the case of official statements, these reports may be intended to sensitise specific target audiences to concrete threat activity and share mitigation and detection measures, while sidestepping the issue of attribution and related expectations about evidence for the involvement of a specific actor or sponsoring nation.

Among the recorded attributions, two statements from the Main Intelligence Department of the Ministry of Defense of Ukraine (GURMO) stand out. GURMO ostensibly issued the statements as an officially uninvolved third party. In both cases, GURMO confirmed pro-Ukrainian hacktivist operations against Russian targets. One case addressed the targeting of a Russian telecommunications company by the IT Army of Ukraine.

A second case addressed activities of the group "BO Team," which was first publicly reported on and was registered for the first time by EuRepoC in January 2024. Given the links between government agencies and the IT Army, a similar setup may be plausible for the BO Team. The extent of the disruptive effects on Russian satellite data processing as described by GURMO, as well as the fact that GURMO had knowledge of the operation, suggests that the operation conducted by BO Team against the Russian space hydrometeorology research centre "Planeta" may have at least been carried out with state connivance, if not participation. GURMO describes BO Team as "voluntary cyber patriots," likely aiming to enhance the group's credibility, reputation, and attention.

Seven recorded cyber operations showed links to conventional conflicts. Six of them were in the context of the Russian war against Ukraine and one was linked to the conflict between Israel and Hamas. This case involved Iranian espionage, more specifically the group Mint Sandstorm (aka APT35), attributed to the Islamic Revolutionary Guard Corps (IRGC). Microsoft reported the group focussed on strategic information related to the current conflict from individuals affiliated with research institutes and universities in Belgium, France, Gaza, Israel, the UK, the US, and Israel. The timing of the espionage campaign aligns with the Israel-Hamas conflict, with the campaign starting in November 2023.

More from EuRepoC

In January, EuRepoC released a new APT profile on the North Korean hacker group Lazarus. The group focuses primarily on cyber espionage in areas of strategic importance to the regime in Pyongyang, as well as operations aimed at financial gain, increasingly targeting the crypto sector. Read more here.

Additionally, EuRepoC published a first empirical analysis of the use of measures from the EU Cyber Diplomacy Toolbox by EU actors, available here.

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