Cyber Brief (March 2026)

April 1, 2026 – Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 343 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, the Council of the European Union sanctioned Chinese and Iranian entities for cyberattacks, while the United States of America (US) sanctioned North Korean IT workers' facilitators. Law enforcement agencies in Europe, together with the US, dismantled the SocksEscort proxy service, and the US Federal Bureau of Investigation (FBI) took down the Iran-linked Handala Hack Team leak site.
- On the **cyberespionage** front, a leak of Russia-linked APT FancyBear exposed its own cyberespionage infrastructure, tools, and data, while a Russia-linked threat actor deployed an iOS full-chain exploit. Additionally, Iran-linked threat actors were observed leveraging cybercrime tooling for state-sponsored operations.
- In regards to **cybercrime**, we observed a proliferation in supply-chain attacks. Cybercrime actor TeamPCP compromised several widely used tools in multi-stage supply-chain attacks, including compromising the Trivy open-source vulnerability scanner, as well as the LiteLLM Python package and the official Telnyx Python package on PyPI. Additionally, a bot called hackerbot-claw began targeting CI/CD workflows in major open-source GitHub repositories.
- In terms of **digital foreign interference**, several campaigns leveraged the ongoing Iran conflict, for example, two Israeli train stations had screens compromised with fake missile warnings, while social media platform X experienced a high volume of disinformation promoting both pro-Iranian and pro-US narratives.
- There were numerous **disruptive and destructive** cyberattacks linked to the ongoing Iran conflict. Handala Hack team, a pro-Iran supposed hacktivist group, claimed a data wiping attack at a US medical company, disrupting global operations. Additionally, pro-Iranian hacktivist group Homeland Justice claimed data wiping attacks on Albania's parliament.
- Regarding **data exposure and leaks**, cybercrime group ByteToBreach reportedly stole Swedish government data from its E-Gov platform. Elsewhere, the Dutch Ministry of Finance reported a breach of its systems in an unspecified cyberattack, and the Dutch national police experienced a breach following a phishing attack.

- As for notable **Common Vulnerabilties and Exposures (CVEs)**, the US Cybersecurity and Infrastructure Security Agency (CISA) reported active exploitation of a critical vulnerability in the Langflow AI workflow framework, and added a VMware Aria Operations RCE flaw to its Known Exploited Vulnerabilities (KEV) catalogue.

For more information regarding CERT-EU's analytical and operational standards to classify, assess, and prioritise malicious cyber activities, please review our Cyber Threat Intelligence Framework here.

Europe

Cyber policy and law enforcement

EU sanctions Chinese and Iranian companies as well as two individuals for cyberattacks
On March 16, the Council of the European Union sanctioned one Iranian and two Chinese companies, plus two individuals, for cyberattacks against EU member states and their partners. The Chinese firms were listed for compromising devices and providing hacking services. The Iranian company was sanctioned for breaching a French subscriber database, advertising disinformation on billboards during the 2024 Paris Olympic Games, and compromising a Swedish SMS service. `sanctions` `china` `iran` link

Europol and international partners disrupt the SocksEscort proxy service
On March 11, Europol, Eurojust, and partners from Europe and the US disrupted the SocksEscort proxy service, which had compromised more than 369.000 routers and IoT devices worldwide. Authorities seized 34 domains and 23 servers, froze 3.5 million US dollars in cryptocurrency, and cut off infected devices used to support cybercrime including ransomware, DDoS attacks, and child sexual abuse material distribution. `law enforcement` link

Cyberespionage & prepositioning

APT28 use custom XSS payloads to compromise e-mail accounts
On March 17, researchers identified exposed infrastructure linked to FancyBear, identifying directories that uncovered tools, stolen data, and campaign details targeting governments and militaries across Europe. The leak showed large-scale credential theft, e-mail exfiltration, and 2FA bypass capabilities, while also highlighting that the group operated carelessly from the same server for over 500 days despite prior public attribution. `public administration` `defence` `russia` link

DarkSword iOS exploit chain adopted by multiple threat actors
On March 18, multiple actors, including commercial surveillance vendor PARS Defense and Russia-linked UNC6353, deployed DarkSword, an iOS full-chain exploit leveraging six vulnerabilities, including zero-days, to fully compromise devices running iOS 18.4–18.7. Victims included targets in Turkey, Ukraine, Saudi Arabia, and Malaysia. Apple has since patched all vulnerabilities. `russia` `psoa` link

China-linked APT Silver Dragon campaign targeting government entities in South-east Asia and Europe
On March 3, China-linked Silver Dragon has been reportedly conducting cyberespionage campaigns against government entities across South-east Asia and Europe since mid-2024. The group exploits public-facing servers and conducts phishing campaigns to gain initial access,

deploying Cobalt Strike beacons, a novel Google Drive-based backdoor, a screen-monitoring implant, and an SSH utility for post-exploitation activity. `public administration` `china` link

Cybercrime

Suspected Qilin ransomware attack disrupts Germany's Left Party infrastructure
On March 27, Germany's Left Party says it detected anomalies in its infrastructure and proactively took systems offline to contain a suspected ransomware attack by the Russian-linked Qilin ransomware group. The party says its infrastructure was affected, with the scope of compromised internal data remaining unclear, but that it had not impacted its member database. It has filed a criminal complaint and is coordinating with security authorities and external experts. `political parties` `civil society` link

Disruption & destruction

Iran-linked hacktivist group claims data wipe at US medical company Ireland offices
On March 11, Iran-linked supposed hacktivist group Handala Hack Team claimed to have wiped about 50TB from over 200.000 systems, servers, and mobile devices at Stryker, a US medical-device company. The attack reportedly disrupted the company's global operations, including disruptions to its office in Cork, Ireland. An unconfirmed statement from the group claimed the cyberattack was retaliation for the airstrike on an Iranian school that killed hundreds of pupils. `health` `iran` link

Iran-linked Homeland Justice cyberattack on Albanian parliament e-mail systems
On March 10, Albania's parliament reported that a cyberattack attempted to delete data and compromise several of its internal systems. The Iran-linked threat actor Homeland Justice claimed responsibility. The attack temporarily suspended internal e-mail services and disrupted access to computers for parliamentary staff and lawmakers. The group stated the attack was retaliation for Albania's hosting of Iranian opposition group Mojahedin-e-Khalq. `public administration` `iran` link

Cyberattack on Poland's National Centre for Nuclear Research likely Iran-linked
On March 12, Polish authorities reported an unsuccessful cyberattack on the National Centre for Nuclear Research, with early indicators pointing to Iranian origins, though officials caution this could be misdirection. According to the Centre, the integrity of the systems was not compromised. The incident followed a separate, confirmed Iran-linked attack on US medical company Stryker, which disrupted Microsoft systems for thousands of employees. `research` `energy` `iran` link

Data exposure and leaks

Cybercrime group ByteToBreach allegedly stole Swedish e-government data and put it up for sale on dark web
On March 13, researchers reported that cybercrime threat actor ByteToBreach allegedly stole Swedish e-government (E-Gov) platform data and put it for sale on the dark web. They claimed to have compromised CGI Sweden, which manages important digital services for several Swedish authorities. The threat actor released the E-Gov source code for free with multiple backup download links, while citizen databases were sold separately. `public administration` link

Cyber attack against the Dutch Ministry of Finance
On March 23, the Dutch Ministry of Finance confirmed that some of its systems were breached in a cyberattack detected on March 19. The breach, identified via a third-party notification, affected an unspecified number of employees. No threat actor has claimed responsibility. Critical services including tax collection, customs, and benefits remained unaffected. The investigation is ongoing and authorities blocked access to compromised systems. `public administration` `finance` link

Phishing attack against the Dutch National Police
On March 25, the Dutch National Police (Politie) reported it had suffered a security breach following a successful phishing attack by an unknown threat actor. The agency's Security Operations Centre detected the incident and blocked the attackers' access. The impact appears limited, with no citizens' data or investigative information exposed. A criminal investigation has been launched. `law enforcement` link

World

Cyber policy and law enforcement

Global Coalition on Telecoms launched to establish voluntary 6G security principles
On March 3, the United Kingdom, US, Canada, Japan and Australia, with Sweden and Finland launched the Global Coalition on Telecoms (GCOT) to establish non-binding security and resilience principles for future 6G networks. The GCOT published a guidance emphasising security-by-design, protection against threats, data confidentiality and integrity, supply-chain resilience, and regulatory compliance. `cybersecurity` `telecommunications` link

Interpol-led operation disrupts cybercrime infrastructure and drives global arrests
On March 13, Interpol-led Operation Synergia III had reportedly sinkholed 45.000 IP addresses and seized servers tied to cybercrime worldwide. The action, carried out with 72 countries between July 2025 and January 2026, led to 94 arrests, 212 seizures and further investigations. Authorities also identified tens of thousands of phishing and fraudulent websites used to steal financial and personal data. `law enforcement` link

International joint action disrupts DDoS botnets
On March 20, a joint global law enforcement operation including the US, Germany, and Canada, disrupted the Aisuru, Kimwolf, Jackskid and Mossad botnets, whose malware droppers infected thousands of devices. Law enforcement agencies seized control servers, arrested suspects and sinkholed domains, halting further infections and data theft. `law enforcement` link

US sanctions entities in multiple countries associated to the North Korean IT workers campaign
On March 12, the US Treasury’s Office of Foreign Assets Control sanctioned a North Korea-based information technology company, a Vietnam-based currency conversion company, and facilitators in Spain, Vietnam, and Laos for enabling the North Korea-linked IT workers campaign. The sanctions reflect North Korean threat actors' use of foreign entities to enable their operations, especially in Vietnam and Laos, which have close diplomatic ties to North Korea. `sanctions` `north korea` link

FBI seized Handala data leak site after Stryker cyberattack
On March 19, the US FBI announced that it seized the Handala data-leak site after it posted files allegedly stolen from Stryker during a cyberattack. The takedown, coordinated with Israeli authorities, follows Handala’s threats to publish 200GB of Stryker data. The seizure banner now

replaces the site, signalling law enforcement action against the group. `law enforcement` `iran` link

Cyberespionage & prepositioning

China-linked UNC2814 cyberespionage operation against Costa Rican Electricity Institute
On March 16, Costa Rica's Electricity Institute, the country's primary provider of electricity and telecommunications services, suffered a cyberespionage intrusion attributed to China-linked UNC2814. Detected in late January 2026, the operation resulted in the extraction of gigabytes of e-mail data. `telecommunications` `energy` `china` link

China-linked Red Menshen BPFdoor implants targeting telecommunications networks
On March 26, a long-term espionage campaign attributed to China-linked threat actor Red Menshen, had reportedly been targeting global telecommunications networks. The group deployed BPFdoor, a covert kernel-level Linux backdoor, to establish persistent access within telecom infrastructure. The campaign aims to enable large-scale intelligence collection, subscriber monitoring, and surveillance of government communications. `telecommunications` `china` link

Iran-linked threat actor targets Iraqi government officials with .NET malware
On March 2, a suspected Iran-nexus threat actor, reportedly conducted a campaign targeting Iraqi government officials back in January 2026. The group impersonated Iraq's Ministry of Foreign Affairs using social engineering lures, including ClickFix-style attacks, to deploy several .NET malware families. Compromised Iraqi government infrastructure was leveraged to host malicious payloads. `public administration` `iran` link

Iran-linked threat actors leveraging cyber criminal ecosystem for state-sponsored operations
On March 10, Iran-linked threat actors, including Handala Hack Team and MuddyWater, were reportedly actively engaging with the cyber criminal ecosystem to support state objectives. Rather than merely mimicking criminal behaviour, these actors are adopting criminal malware, ransomware affiliate programmes, and shared infrastructure. Targets include Israeli and Albanian entities, with notable attacks against Israeli hospitals and organisations across government, defence, and telecommunications sectors. `health` `defence` `public administration` `telecommunications` `iran` link

Israeli military QR code leaflet campaign targeting Lebanese civilians
On March 13, Israel's air force reportedly dropped thousands of leaflets over Beirut containing QR codes linked to WhatsApp and Facebook contacts. Lebanese authorities and cybersecurity experts warned citizens against scanning the codes, citing risks of device compromise, identity exposure, and phishing. `israel` link

Cybercrime

Hackerbot-claw CI/CD workflow exploitation and token theft campaign
On March 1, an automated campaign by a bot dubbed Hackerbot-claw began targeting CI/CD workflows in major open-source GitHub repositories. The bot opened multiple pull requests to trigger vulnerable automation and gain code execution, including theft of a GitHub token with write access. It targeted at least seven projects, with several compromised, and one incident led to a full-repository takeover and downstream supply chain risk. `cybersecurity` `technology` link

Supply-chain compromise of Trivy vulnerability scanner
On March 20, a researcher reported that threat actor TeamPCP compromised the Trivy open-

source vulnerability scanner in a supply-chain attack, backdooring an official release and tampering with associated GitHub Actions. Using previously stolen credentials, attackers distributed credential-stealing malware targeting developer and CI/CD environments globally. Stolen data was exfiltrated to an attacker-controlled server. The same actor was linked to a follow-up campaign deploying a self-propagating npm worm named CanisterWorm. `technology` link

LiteLLM PyPI supply chain compromise by TeamPCP
On March 24, the threat actor TeamPCP reportedly compromised the popular LiteLLM Python package on PyPI, publishing malicious versions 1.82.7 and 1.82.8. The backdoored packages deployed a credential-stealing payload harvesting SSH keys, cloud tokens, Kubernetes secrets, and environment variables, exfiltrating data to attacker-controlled infrastructure. Approximately 500.000 devices were reportedly affected globally. Both malicious versions have since been removed from PyPI. `artificial intelligence` `technology` link

TeamPCP supply-chain attack on Telnyx PyPI package
On March 27, threat actor TeamPCP reportedly compromised the official Telnyx Python package on PyPI, uploading malicious versions 4.87.1 and 4.87.2. The backdoored packages delivered credential-stealing malware hidden within WAV audio files using steganography. On Linux and macOS, the malware harvested SSH keys, cloud tokens, and credentials; on Windows, it established persistence. With over 740.000 monthly downloads, the package's wide adoption poses a significant global supply-chain risk. `technology` link

Digital foreign interference

Israeli cyber authorities received 1.300 reports of intimidation calls and messages targeting civilians since the start of Iran conflict
On March 10, Israeli media reported that Israel's National Cyber Directorate had received approximately 1.300 civilian reports of intimidation calls and messages since February 28, with many messages also seeking personal information. The reporting aligns with a broader pattern of wartime social-engineering activity exploiting fear, urgency and trusted civic messaging to pressure civilians. `civil society` `iran` link

Israeli train station screens compromised with fake missile warning messages
On March 12, unknown threat actors compromised digital advertising signs at two Israeli train stations to display false warnings of an incoming missile attack. The screens were quickly taken offline. Earlier on the same day, Iranian media falsely claimed that Israel's entire railway system was hacked and disabled. However, railway officials stated the screens were not connected to railway infrastructure, and presented no risk to infrastructure or passenger information. `transportation` `iran` link

X disinformation surge using recycled and AI-altered Iran attack media
On February 28, the social media platform X experienced a spike in disinformation after the initial US and Israeli military strikes on Iran. Posts included recycled footage, misattributed locations, AI-altered images, and video game clips. Blue-check accounts amplified false claims about missile strikes and downed jets, while pro-Iranian and pro-Trump accounts spread misleading narratives. Posts gained millions of views, shaping public perception despite later corrections. `social media` `iran` `united states` link

Disruption & destruction

Iranian regime imposes nationwide internet blackout amid US and Israel strikes
On March 2, the Iranian regime reportedly imposed a nationwide internet blackout amid US and

Israeli military airstrikes. Connectivity dropped from partial disruption to near-total outage, flatlining around 1% of ordinary levels for over 48 hours. The shutdown limited communications and visibility into events on the ground, affecting the country's population at a national scale. `telecommunications` `iran` link

Notable CVEs

Active exploitation of critical Langflow vulnerability enabling AI workflow hijacking
On March 26, CISA reported active exploitation of CVE-2026-33017, a critical vulnerability in the Langflow AI workflow framework. The flaw allows unauthenticated remote code execution via crafted HTTP requests, with exploitation beginning within 21 hours of public disclosure. Attackers have been observed harvesting sensitive data including environment and database files. CISA has added the vulnerability to its KEV catalogue, urging immediate patching. `artificial intelligence` link

VMware Aria Operations RCE flaw CVE-2026-22719 exploited in the wild
On March 3, CISA added VMware Aria Operations RCE flaw CVE-2026-22719 to its KEV catalogue. This vulnerability allows a remote attacker to execute arbitrary commands on the affected systems, which could result in unauthorised access, system compromise, and disruption of services. Broadcom stated that it can only be exploited during support-assisted product migrations. link

1. Conclusions or attributions made in this document merely reflect what publicly available sources report. They do not reflect our stance.

TLP definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and its clients.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
CLEAR	Disclosure is not limited.	TLP:CLEAR information may be distributed freely.