# Cyber Security Brief (February 2024)

*March 1, 2024 - Version: 1.0*

**TLP:CLEAR**

*Disclosure is not limited.*

*TLP:CLEAR information may be distributed freely.*

## Executive summary

- We analysed 272 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, the EU urges major tech platforms to identify AI-generated content to safeguard upcoming elections from disinformation. A global coalition comprising the UK, France, the US, and leading tech firms will tackle proliferation and irresponsible use of commercial cyber intrusion tools and services. International law enforcement agencies, including Europol and the FBI, conducted operations to dismantle cybercriminal networks involved in distributing ransomware (LockBit) and malware (Warzone RAT), resulting in arrests, server seizures, and disruption of criminal infrastructure. Law enforcement authorities disrupted botnets operated by the China-linked Volt Typhoon and Russia-linked APT28 threat actors, targeting critical infrastructure in the US and conducting cyber attacks globally.
- On the **cyberespionage** front, I-Soon, a Chinese contractor for PRC agencies, was exposed for conducting offensive cyber activities, the Dutch Ministry of Defence attributes a cyberattack in 2023 to a Chinese state-sponsored actor, Germany and South Korea warn of North Korean threat actors targeting the defence sector globally. There was also reporting of cyberespionage activities by Russian, North Korean and Iranian groups as well as new evidence of use of private sector offensive actor spyware.
- Relating to **cybercrime**, a ransomware attack affected over 100 healthcare facilities in Romania, while the LockBit ransomware resumed operations, threatening governments, after facing setbacks. In Europe, the top 5 most active ransomware operations have been Lockbit3, Qilin, 8Base, Hunters and Lockbit3-cronos and the top 5 most targeted sectors have been manufacturing, technology, civil society & non-profits, construction & engineering and hospitality.
- There were **disruptive** attacks with the Iranian threat actor Cotton Sandstorm reportedly disrupting UAE TV with a deepfake report, and hackers targeting Israeli flights' communications over the Middle East, prompting safety concerns.
- About **information operations**, in Europe, a Russia-aligned PSYOPs, uncovered by ESET, aimed to demoralise Ukrainians with false war-related information, while Doppelgänger, a suspected

Russia-linked cluster, intensified targeting German audiences, raising concerns about election interference. Meanwhile, Citizenlab exposed Paperwall, a Chinese-operated network disseminating pro-Beijing disinformation across 30 countries, adding to the region's information warfare landscape.

- We noticed significant **data exposure and leaks** incidents in the health, education, social media and technology sectors.
- On the **hacktivism** front, pro-Russia hackers launched DDoS attacks against Finland and Denmark in response to their support for Ukraine, while also targeting a Maltese newspaper for its stance on Russian sanctions. Meanwhile, the Turkish Hack Team threatened to revive its #OpSweden campaign following a Quran-burning incident in Stockholm.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in February 2024.

# Europe

## Cyber policy and law enforcement

**European Commission recommends replacement of high-risk suppliers in Europe's submarine cable network**
On February 21, the European Commission proposed a gradual replacement of high-risk suppliers for submarine cables, emphasising the need to bolster security and reliability in Europe's telecommunications infrastructure by mitigating potential vulnerabilities associated with certain suppliers. *Risk management*

**EU turns to technology companies to help deepfake-proof election**
In a statement made before EU lawmakers in early February, Internal Market Commissioner Thierry Breton emphasised the necessity for major tech platforms like TikTok, X, and Facebook to soon identify AI-generated content. This measure aims to safeguard the upcoming European election from disinformation. The timeline for implementing content labelling under the EU's Digital Services Act (DSA) was not provided. *Artificial intelligence*

**Global coalition against malicious spyware**
On February 6, the UK, France, and the United States, alongside technology firms including Google, Microsoft, and Meta, have agreed on a joint statement to combat the malicious use of cyber spying tools. This commitment, endorsed by 35 nations at a conference co-hosted by the UK and France, is to tackle proliferation and irresponsible use of commercial cyber intrusion tools and services. *Cooperation*

**Albanian government strengthens cybersecurity amid threats from Iran and Russia**
On February 19, the Albanian government passed a new cybersecurity bill, aiming to bolster the country's cybersecurity infrastructure in response to cyber threats from Iran and Russia. The bill includes provisions for establishing a national cybersecurity centre, increasing training budgets, and giving oversight to critical infrastructure, with an emphasis on enhancing defences against sophisticated cyberattacks targeting critical infrastructure and state entities. *Legislation*

**Denmark orders schools to stop sending student data to Google**
Denmark's data protection authority has ordered 53 municipalities to change how they transfer student data to Google after concerns were raised about privacy and legality. *Data protection*

**Disruption of APT28's GRU-operated botnet**
On February 27, European and other international partners and peers released a joint cybersecurity advisory on the disruption of a botnet controlled by the Russian General Staff Main

Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS), also known as APT28. As early as 2022, APT28 threat actors had utilised compromised EdgeRouters to facilitate covert cyber operations against governments, militaries, and organisations around the world. *Take dowm*

**Europol disrupts LockBit ransomware operation as part of a joint international law enforcement operation**
On February 19, an international operation led by the UK National Crime Agency, in coordination with Europol and Eurojust under Operation Cronos, targeted the LockBit criminal organisation. It resulted in the takedown of 34 servers, arrests in Poland and Ukraine, and the freezing of over 200 cryptocurrency accounts. The UK's National Crime Agency now controls LockBit's infrastructure and darkweb site. LockBit is notorious for causing billions of euros worth of damage as one of the world's most prolific ransomware. *Take down*

**Europol and FBI take down Warzone malware**
On February 7, an international operation led by the FBI, supported by Europol, seized internet domains used by cybercriminals to distribute the Warzone RAT malware. Two suspects were arrested for selling the malware, with Europol aiding the investigation involving cooperation from multiple countries to secure servers hosting the malware infrastructure. *Take down*

**Spanish National Police arrest suspect for massive vehicle data breach**
On February 27, the Spanish National Police arrested a suspect accused of stealing data related to over 40 million vehicles, initiating an investigation into data breaches dating back to 2020, allegedly exploiting vulnerabilities in property-tax web forms across various autonomous communities. The arrest led to the recovery of the suspect's database and backups, with collaboration from multiple agencies, while the data stolen remain undisclosed. *Arrest*

# Cyberespionage

**I-Soon leak reveals private Chinese company conducting offensive cyber activity for the Chinese government**
Over the weekend of February 16, I-Soon, a Chinese company contracted by multiple PRC agencies, experienced a data leak. I-Soon appears to conduct offensive cyber activity for the Chinese government. The documents revealed an eight-year effort to target databases and tap communications across Europe and Asia. The files also revealed a campaign to monitor the activities of ethnic minorities in China and target online gambling companies. *Chinese threat actor*

**Dutch government publicly attributes a cyberattack on its Ministry of Defence to a Chinese state-sponsored actor**
On February 6, the Dutch government, via NCSC-NL, released an advisory revealing an incident from 2023 that targeted the Dutch Ministry of Defence. Dutch intelligence services attribute the attack with high confidence to a state-sponsored actor from China. The intrusion utilised a newly identified implant named COATHANGER and exploited a heap-based buffer overflow vulnerability (CVE-2022-42475) in FortiOS SSL-VP. The breach impacted a Dutch military research and development server. *Chinese threat actor*, *Defence*

**German and South Korean report about North Korean threat actors targeting the defence sector**
On February 19, the Bundesamt für Verfassungsschutz (BfV) of the Federal Republic of Germany and the National Intelligence Service (NIS) of the Republic of Korea (ROK) issued a joint security advisory, warning of North Korean threat actor campaigns targeting the defence sector globally. These campaigns focus on defence companies and research centres, exemplified by two distinct methods: a supply-chain attack since late 2022 and a social engineering campaign since mid-2020, known as Dream Job, which is likely ongoing. *North Korean threat actor*, *Defence*

**Callisto targets researchers of think tanks**
Recorded Future reported on February 1 about a campaign by the Russian group Callisto which

targeted academics in the UK and the US, members of think tanks. The attackers targeted researchers critical of the Kremlin, attempting to breach email accounts and gather intelligence that could be used to discredit them. *Russian threat actor*

**Polish PM says previous ruling party used Pegasus spyware against 'very long' list of victims**
Poland's new prime minister, Donald Tusk, claimed to have uncovered proof that the previous government illegally used Pegasus spyware to surveil numerous targets. This revelation, made during a meeting with President Andrzej Duda, on February 13, follows a Polish Senate investigation that found constitutional violations during the 2019 elections due to Pegasus use. Tusk's allegations echoed concerns about spyware misuse in other European countries. *Private sector offensive actor*

**Politico reports MEPs infected with spyware**
On February 21, Politico reported that several members of the European Parliament subcommittee on security and defence (SEDE) have had their phones hit with intrusive surveillance software tools. All members of the subcommittee have been advised to take their phones to the institution's IT service to be checked for spyware. *Unattributed threat actor*

**UAC-0184 targets Ukrainian entity in Finland with Remcos RAT**
Morphisec Threat Labs analysis revealed that threat actor UAC-0184 has been utilising steganography to distribute the Remcos remote access Trojan (RAT) via a new malware called IDAT Loader to a Ukrainian entity in Finland. Their end goal was cyberespionage. Researchers have noted parallel campaigns by UAC-0148, allegedly involving email and spearphishing, offering job opportunities to Ukrainian military personnel for consultancy roles with the Israel Defense Forces (IDF). *Unattributed threat actor*

## Cybercrime

**Ransomware attack criples Romanian hospitals**
On February 12, at least 100 hospitals in Romania were hit by the Backmydata ransomware variant, causing their healthcare systems to shut down. The attack targeted the Hipocrate Information System (HIS), disrupting medical activities and patient data management. The Romanian Ministry of Health confirmed the attack and investigations are ongoing. *Ransomware, Health*

## Information operations

**Russian-made PSYOPs in Ukraine: Operation Texonto**
On February 21, 2024, ESET Research uncovered Operation Texonto, a Russian-aligned disinformation campaign distributing spam e-mails to influence and demoralise Ukrainian citizens with false war-related information. The campaign consisted of two waves in November and December 2023. Additionally, ESET detected spearphishing attacks in October and November 2023 targeting a Ukrainian defence company and an EU agency, aiming to steal Microsoft Office 365 credentials. Similar network infrastructure links these operations. *Russian threat actor*

**Doppelgänger, a suspected Russia-linked group seen intensively targeting Germany**
On February 22, researchers from Sentinel Lab released findings about a disinformation campaign led by Doppelgänger, a suspected Russia-linked information operation cluster. They report that they have seen the group intensively targeting German audiences. The German Ministry of Foreign Affairs highlights a growing concern about election interference, both in municipal, federal state, and European Parliament elections this year, as well as federal government elections next year. *Russian threat actor*

**PAPERWALL: Chinese websites posing as local news outlets target global audiences with pro-Beijing content**
According to a report published by Citizenlab on February 5, a network of at least 123 websites operated from within the People's Republic of China while posing as local news outlets in 30 countries across Europe, Asia, and Latin America, disseminates pro-Beijing disinformation and ad hominem attacks within much larger volumes of commercial press releases. Citizenlab names this campaign PAPERWALL. *Chinese threat actor*

**Deepfake operation targeted Romania's longest-serving central bank governor in disinformation campaign**
Romania's longest-serving central bank governor, Mugur Isarescu, was impersonated in a deepfake video promoting bogus investments. This incident, part of a broader disinformation operation also targeting the Prime Minister, led the National Bank of Romania to announce and clarify on February 5 that it does not offer investment advice, emphasising the misuse of Isarescu's trusted image to deceive the public. *Unattributed threat actor*

## Data exposure and leaks

**Data breaches at Viamedis and Almerys impact 33 million in France**
In early February, Viamedis disclosed a cybersecurity incident on LinkedIn, reporting a data breach affecting beneficiaries and healthcare professionals. Along with a breach at Almerys, over 33 million individuals in France are now affected. Viamedis and Almerys manage sensitive healthcare and insurance data, handling reimbursement and transactions within France's insurance system. *Health*

**Danish IT firm Netcompany suffers a data leak**
On February 23, Version 2, a Danish news website focusing on technology, reported that a group called Zyndicate claimed to have leaked data from Denmark's Netcompany, including source code, scripts, and passwords. Netcompany confirmed the incident but denied that the leaked data allows access to programs and databases. Cybersecurity experts found much of the leaked content targeting Danish government entities. Zyndicate indicates having been able to breach the Danish government. *Technology*

## Hacktivism

**Russian hackers attack Finland for supporting Ukraine**
On February 1, a Telegram post by @noname05716 announced DDoS attacks on Finnish government services by eight cyber threat actors, led by the hacktivist group NoName057(16). The attacks were in response to Finland's support for Ukraine and perceived anti-Russian policies. They affected 40 entities in Finland and gained traction on Russian and Belarusian Telegram channels. *Russian threat actor*

**NoName057(16) targets Danish websites in response to Denmark's support for Ukraine**
Since February 23, pro-Russia hacktivist group NoName057(16) claimed to have conducted DDoS attacks against at least 20 Danish websites of financial services, transportation, and government entities, citing Denmark's recent 10-year commitment to supporting Ukraine. On February 26, Cyber Army of Russia also claimed DDoS attacks against Danish targets, coinciding with Denmark's alignment with other European countries in providing long-term support to Ukraine. *Russian threat actor*

**Russian hacktivist attack on Maltese newspaper**
A group of Russia-linked cybercriminals claimed responsibility for a major attack on the Times of Malta website, allegedly in retaliation against Malta's support of sanctions against Russia. The

People's Cyber Army of Russia urged its followers on Telegram to target the Times of Malta, resulting in a DDoS attack, on February 8, that overwhelmed the website's servers and forced it offline for around 45 minutes. Although no data breach occurred, the attack prompted the newspaper to report the incident to the police. *Russian threat actor*

**Türk Hack Team threatens #OpSweden revival after Quran-burning incident**
Since February 19, Türk Hack Team (THT) has threatened to revive its #OpSweden campaign following a Quran-burning demonstration in Stockholm, intending to conduct DDoS attacks and hack-and-leak operations against Swedish and unspecified EU entities, with potential collaboration from other hacktivist groups. The announcement comes amid group's frustration with the Swedish government's response to anti-Islam activities. *Turkish threat actor*

# World

# Cyber policy and law enforcement

**US announces visa restriction policy applicable to those misusing commercial spyware**
On February 5, the US introduced a new visa restriction policy targeting individuals associated with the inappropriate use of commercial spyware. This includes spying on or intimidating activists, political dissidents, vulnerable populations, or marginalised communities, as well as their family members. The policy applies to those directly involved in misuse and those who facilitate or profit from it, such as investors or operators of companies supplying spyware to governments or their representatives. *Sanctions*

**UN claims North Korea behind cyber attacks worth 3 billion US dollars**
UN sanctions monitoring team reported on February 7 that North Korea is suspected of carrying out cyberattacks, allegedly earning 3 billion US dollars for its nuclear weapons program. The attacks, attributed to hacking groups linked to Pyongyang's intelligence agency, continue despite sanctions. North Korea also evades sanctions through illicit financial operations. *Sanctions*

**US government releases information on how to secure water systems better**
On February 21, the US government released a Fact Sheet for the water and waste water systems sector with top actions to secure operational technology (OT) and information technology (IT) water systems from cyberattacks. The information is aimed at reducing the risk and improve the resilience of water systems to malicious cyber activity. *Policy*

**FCC orders telecom carriers to report personal data breaches within 30 days**
Starting March 1, telecom companies in the US must report data breaches affecting customers personally identifiable information within 30 days, following Federal Communications Commission (FCC)'s updated reporting requirements. The rule aims to modernise breach notification rules to ensure timely notification to customers, holding providers accountable for safeguarding sensitive information. *Policy*

**US FTC proposes ban on Avast's sale of user browsing data amid record fine**
On February 21, the US FTC proposed banning UK-based software company Avast Limited and its subsidiaries from selling users' browsing data to third parties, alleging violations from 2014 to 2020. Avast reportedly sold web browsing data to over 100 companies through its subsidiary Jumpshot, resulting in a proposed 16,5 million US dollar fine, the highest in a privacy-violation case. *Ban*

**Biden's executive order prohibits bulk sale of Americans' data to China and Russia**
On February 28, US President Joe Biden issued an executive order banning the mass sale and transfer of Americans' private data to countries including China and Russia, citing national

security concerns, while Attorney General Merrick B. Garland emphasised the need to protect sensitive personal data from being exploited for malicious activities. *Data protection*

**US offers 10 million US dollars for tips on Hive ransomware leadership**
In early February, the US State Department announced offering up to 10 million US dollars in rewards for information on the Hive ransomware gang, which extorted around 100 million US dollars from over 1.300 companies across 80 countries between June 2021 and November 2022, according to the FBI. *Bounty*

**Former CIA officer sentenced to 40 years for CIA data breach**
On February 1, the US Department of Justice (DOJ) announced former Central Intelligence Agency (CIA) officer Joshua Adam Schulte has been sentenced to 40 years in prison for a series of crimes including espionage, computer hacking, and the largest data breach in CIA history, with his transmission of stolen data to WikiLeaks marking one of the largest unauthorised disclosures of classified information in the US. *Sentence*

**Interpol operation Synergia disrupted a cybercrime infrastructure**
On February 1, Interpol reported on an international law enforcement operation named Synergia which successfully dismantled more than 1.300 command and control (C2) servers, which were crucial for orchestrating ransomware, phishing, and malware campaigns. Most of those servers were located in Europe and enabled cybercriminals to control infected devices remotely, facilitating further malicious activities and data theft. *Take down*

**FBI disrupts KV Botnet used by China-linked Volt Typhoon**
On January 31, the FBI announced in a press conference that they disrupted the KV Botnet used by China-linked threat actor Volt Typhoon, namely used to hijack small office/home offices (SOHO) in the United States to ultimately target critical infrastructure. *Take down*

**FBI disrupts APT28 botnet**
On February 15, the FBI dismantled a botnet composed of small office/home office routers used by the Russian group APT28 to facilitate cyber attacks against the US and its allies. The botnet included hundreds of Ubiquiti Edge OS routers infected with Moobot malware and was utilised for spearphishing and credential theft, targeting governments, military, and corporate organisations globally. The Moobot malware was originally deployed by cybercriminals and was repurposed for espionage. *Take down*

# Cyberespionage

**Five Eyes warn of Russian APT29 shift to cloud attacks**
On February 26, the Five Eyes intelligence alliance issued a warning stating that Russia's Foreign Intelligence Service, APT29, have shifted their focus to attacking cloud services, utilising various sophisticated methods including stolen credentials and dormant accounts to gain access. *Russian threat actor*

**APT28 uses brute force to target multiple sectors**
According to TrendMicro, from approximately April 2022 until November 2023, the Russia-linked APT28 (also known as Pawn Storm and Forest Blizzard) threat actor, attempted to launch NTLMv2 hash relay attacks through different methods. The victims of these campaigns include organisations dealing with foreign affairs, energy, defence, and transportation. *Russian threat actor*

**QiAnXin identified APT29 targeting Asian energy and chip sectors**
According to QiAnXin, a Chinese cybersecurity company, the Russia-linked APT29 threat actor (that they track as APT-Q-77) targeted China's semiconductor and energy sectors in 2023, with a

keen interest in Central, North, and Southeast Asian projects. QiAnXin revealed this activity in their global APT threat landscape report released on February 2. *Russian threat actor*

**Russian government software compromised to deliver Konni RAT malware by North Korean actors**
On February 22, German cybersecurity firm DCSO discovered that a software installer, called Statistika KZU, utilised by the Russian Consular Department of the Ministry of Foreign Affairs (MID) was compromised to disseminate the Konni RAT malware, attributed to North Korean actors. The installer is meant for transmitting annual report files from foreign consular posts to the MID's Consular Department. *North Korean threat actor*

**New malicious PyPI packages used by North Korean Lazarus threat actor**
On February 28, JPCERT/CC reported that Lazarus distributed malicious Python packages through PyPI, the official Python package repository. The package names, `pycryptoenv` and `pycryptoconf`, closely resemble `pycrypto`, a Python package utilised for encryption algorithms in Python. Hence, the malicious packages containing malware were likely crafted to exploit users' typing errors during Python package installations. The confirmed malicious Python packages have been downloaded around 300 to 1.200 times. *North Korean threat actor*

**North Korean hackers targeting developers with malicious npm packages**
On February 20, Phylum, a software supply chain security company, identified suspicious npm packages on the Node.js repository. These packages, such as `execution-time-async` contain scripts for cryptocurrency mining and credential theft. Additionally, four similar packages have been discovered, totalling 325 downloads. The connection to North Korea stems from the resemblance of the JavaScript code in these packages to BeaverTail malware, associated with North Korean threat actors. *North Korean threat actor*

**Mustang Panda suspected of targeting Myanmar Ministry of Defence and Foreign Affairs**
According to a report released on January 23 by CTI-CSIRT, the China-linked threat actor Mustang Panda is suspected to have targeted Myanmar's Ministry of Defence and Foreign Affairs between November 2023 and January 2024. It is likely they executed two campaigns with the goal of deploying backdoors and remote access trojans. *Chinese threat actor*

**Chinese state-sponsored actors compromise and maintain persistent access to US critical infrastructure**
On February 7, the US CISA released a cybersecurity advisory with Five Eyes partner organisations disclosing details of a China-nexus state-sponsored cyber group known as Volt Typhoon (also known as Vanguard Panda, Dev-0391, UNC3236, Voltzite, and Insidious Taurus) activity. The threat actor is reportedly targeting US-based entities within the energy, telecommunications, transportation, and water and wastewater systems sectors. *Chinese threat actor*

**Earth Lusca exploits geopolitical tensions to target Taiwan ahead of elections**
Between December 2023 and January 2024, TrendMicro traced a campaign by the Earth Lusca threat actor exploiting Chinese-Taiwanese tensions through social engineering. They used spearphishing e-mails discussing Taiwan's geopolitics during national elections, employing multistage infection methods, ultimately delivering a Cobalt Strike payload. Leaked data hinted at a possible collaboration with the Chinese company I-Soon. *Chinese threat actor*

**Classified Japanese diplomatic info leaked after 2020' Chinese cyberattacks**
According to Japan Times article published on February 5, classified Japanese diplomatic information was leaked in 2020 due to Chinese cyberattacks on the Foreign Ministry. The attack, detected during Prime Minister Shinzo Abe's tenure, involved the release of highly confidential diplomatic telegrams exchanged between the ministry and foreign missions. Tokyo and Washington discussed countermeasures in response to the breach. *Chinese threat actor*

**Suspected Iranian espionage targeting aerospace and defence sectors in the Middle East**
On February 27, Mandiant reported that the suspected Iranian threat actor UNC1549 is targeting aerospace and defence sectors in the Middle East, including Israel and the UAE. Their espionage activities, linked to the Tortoiseshell activity cluster and potentially the IRGC, employ evasion techniques such as Azure cloud infrastructure and social engineering for backdoor dissemination. *Iranian threat actor*

**Iranian actor APT42 attacks international targets**
On February 14 Volexity reported that the Iranian-origin threat actor APT42 (a.k.a. Charming Kitten) has launched a sophisticated cyber espionage campaign targeting international figures in journalism, think tanks, and NGOs. They used social engineering and phishing tactics to install malicious VPN applications. They then deployed various pieces of malware for data theft. The campaign is notable for its complexity and focuses on political intelligence. *Iranian threat actor*

**Pegasus spyware intrusions found in civil society members of Jordan**
On February 1, an internet advocacy group called Access Now reported that they had identified spyware intrusions linked to the Pegasus spyware on mobile devices of at least 35 Jordanian civil society members. These include at least one local politician, four non-governmental organisation representatives, 16 journalists and media professionals, five activists, and one IT professional. *Private sector offensive actor*

**NBC News claims US cyberespionage towards Iranian spy ship**
On February 14, 2024, NBC News reported that according to three US officials, a cyberattack was reportedly carried out by the United States on a suspected Iranian spy ship. The supposed cyberattack took in the first week of February as part of a government response to a drone attack by Iranian-backed militias in Iraq that killed three US service members in Jordan. *United States threat actor*

**OpenAI bars several state threat actors from using ChatGPT**
OpenAI, the company behind ChatGPT, reported on February 15, that they collaborated with Microsoft to disrupt five state-affiliated threat groups from China, Iran, North Korea, and Russia. These actors used OpenAI services for various purposes such as researching companies, translating technical papers, scripting support, and drafting content for phishing campaigns. Despite efforts to minimise misuse, OpenAI acknowledged the ongoing challenge posed by malicious actors. *Chinese threat actor*, *Russian threat actor*, *North Korean threat actor*, *Iranian threat actor*

## Cybercrime

**LockBit ransomware resumes operations on new infrastructure**
Since February 25, LockBit ransomware resumed operations on new infrastructure after being disrupted by law enforcement, announcing plans to target government sectors more aggressively. Despite restoring servers and addressing vulnerabilities, LockBit faces challenges in restoring trust between affiliates and stakeholders due to the recent setback and potential data breaches. *Ransomware*

**Crime campaign targeting MS Azure accounts**
On February 12, Proofpoint researchers revealed a cloud account takeover campaign targeting Microsoft Azure environments. Hundreds of user accounts, including senior executives, were compromised using a combination of credentials and personalised phishing lures in shared documents. The campaign affects diverse roles across global organisations, suggesting a broad targeting approach. Post-compromise activities suggest cybercrime motives, with potential Russian and Nigerian involvement, though the origin remains uncertain. *Cloud*

**Prudential Financial breached in data theft cyberattack**
On February 12, Prudential Financial, a major global financial services firm with 1,4 trillion US dollars in assets, disclosed a breach last week. Attackers accessed employee and contractor data before being halted. The breach was detected on February 5, suspected to be by a cybercrime group. The case was reported in an 8-K form filed with the SEC. *Finance*

**Bank of America warns customers of data breach after vendor hack**
In early February, Bank of America warned of a data breach from a hack on one of its service providers, Infosys McCamish Systems (IMS). Personal data of customers, including names, addresses, and financial data, was exposed. IMS reported 57.028 affected individuals. The breach occurred on November 3, 2023, with the LockBit ransomware gang claiming responsibility. *Banking*

## Data exposure and leaks

**Misconfiguration in learning app exposes data of more than 2 million users**
On February 7, industry researchers revealed that a misconfigured MongoDB database for the learning app LectureNotes exposed personal data of over 2 million users. The exposed data includes usernames, names, e-mail addresses, encrypted passwords, phone numbers, IP addresses, user-agent strings, session tokens, and some administrator information such as authorisation IDs and secrets. LectureNotes facilitates peer-to-peer note-sharing among students, faculties, and institutions. *Education*

**Global network service provider exposes DB containing 380 million records**
A cybersecurity researcher discovered, on February 15, an unprotected database with 380 million records, including customer data, belonging to the global network service provider Zenlayer. The researcher notified Zenlayer, but received no response. The database exposed customer information, server logs, internal emails, and VPN records. *IT*

**200.000 Facebook Marketplace user records leaked on hacking forum**
In mid-February, a threat actor leaked 200.000 records on a hacker forum, claiming they contained personal information of Facebook Marketplace users. BleepingComputer verified some data, matching email addresses and phone numbers. IntelBroker, the threat actor, claims the data was stolen after hacking a Meta contractor's systems in October 2023. *Social media*

## Information operations

**Meta disables account linked to Iran's supreme leader**
On February 8, Meta removed Instagram and Facebook accounts linked to Iran's Supreme Leader Ayatollah Ali Khamenei for promoting Hamas, designated as a terrorist group. This was due to repeated violations of Meta's policy on Dangerous Organizations Individuals. Khamenei had endorsed Hamas attack on Israel in October. Despite being blocked in Iran, Khamenei's office maintains social media accounts, including a Persian Instagram account with over 5 million followers. *Iran*

## Disruption

**Iranian group interupts UAE TV to broadcast deepfake report**
On February 8, Microsoft linked the Iranian group Cotton Sandstorm to disrupted TV streaming services in the UAE. The broadcast featured a deepfake news report on the Gaza war, utilising AI-generated elements. The hack also affected channels in Canada and the UK, marking Iran's first major use of AI in influence operations. *Iranian threat actor*

**Attempt to disrupt Israeli flights' communications**
On February 18, the Jerusalem Post reported that hackers had targeted two Israeli flights that were flying over the Middle East and tried to influence the planes' communications networks to divert them from their routes. The pilots reportedly ignored the suspicious instructions and safely flew the planes to their destination. The Jerusalem Post says the incident took place while the planes flying over an area where the Iran-backed Houthis are active. *Unattributed threat actor*

## Significant vulnerabilities

**High Vulnerability in the runc package**
A critical vulnerability has been identified in all versions of runc package up to and including 1.1.11, affecting Docker, Kubernetes, and other containerisation technologies. This vulnerability, tracked as "CVE-2024-21626" with a CVSS score of 8.6, enables attackers to escape containers and potentially gain unauthorised access to the host operating system. See CERT-EU's SA 2024-16.

**Critical Vulnerabilites in FortiSIEM**
In February 2024, Fortinet quietly updated a 2023 advisory, joining two critical flows to the list of OS Command vulnerabilities affecting its FortiSIEM product. If exploited, these vulnerabilities could allow a remote unauthenticated attacker to execute commands on the system. Updating is recommended as soon as possible. See CERT-EU's SA 2024-17.

**Critical Vulnerabilities in FortiOS**
On February 9, 2024, Fortinet released an advisory regarding critical vulnerabilities affecting FortiOS that, if exploited, would allow a remote and unauthenticated to execute code on the affected device. One of the critical vulnerabilities is potentially being exploited in the wild. It is recommended updating as soon as possible. See CERT-EU's SA 2024-18.

**Critical Vulnerabilities in Microsoft Products**
On February 13, 2024, Microsoft released its February 2024 Patch Tuesday advisory, addressing 73 vulnerabilities, two of which are exploited in the wild. See CERT-EU's SA 2024-19.

**Critical Vulnerability in Zoom Products**
On February 13, 2024, Zoom released a security advisory addressing one critical vulnerability. If exploited, this vulnerability allows an unauthenticated attacker to conduct privilege escalation on the target system via network access. See CERT-EU's SA 2024-20.

**Vulnerabilities in Atlassian Products**
On February 20, 2024, Atlassian released a security advisory addressing a high severity vulnerability in Confluence Data Center and Confluence Server that, if exploited, could allow an authenticated attacker to execute arbitrary HTML or JavaScript code on a victim's browser. The security advisory also addresses 10 other high severity vulnerabilities which have been fixed in new versions of several Atlassian products. See CERT-EU's SA 2024-21.

**Vulnerabilities in Adobe products**
On February 13, 2024, Adobe released two security advisories addressing multiple high severity vulnerabilities in various Adobe products. If exploited, the vulnerabilities would allow an attacker to cause remote arbitrary code execution, remote denial of service, remote code injection or disclosure of sensitive information. See CERT-EU's SA 2024-22.

_All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories/_`

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 | Limited disclosure, restricted to participants' organisations and their clients. | Recipients may share TLP:AMBER information only with members of their own organisation and it's clients. |
| AMBER+STRICT | Limited disclosure, restricted to participants' organisations. | Recipients may share TLP:AMBER+STRICT information only with members of their own organisation. |
| 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. |