Cyber Security Brief (March 2024)

April 3, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 245 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, in Europe the Council presidency and the European Parliament reached an agreement on the Cyber Solidarity Act to enhance EU cyber resilience and cooperation, and Germany dismantled two major darknet platforms, Crimemarket and Nemesis. The UN General Assembly adopted a resolution to balance AI development with human rights protections while the US introduced legislation mandating the labelling of AI-generated content. The US sanctioned individuals and entities involved in cyberespionage and disinformation campaigns, including those from China, Russia, and associated with Predator spyware.
- On the **cyberespionage** front, supposedly Russia and China linked threat actors were active in Europe. One of the attacks was the targeting of German political parties by the APT29 threat actor. On the global level, cybersecurity companies and governments reported cyberespionage operations by allegedly Chinese, Russian, Iranian, North Korean threat actors as well as from private sector offensive actors (PSOAs).
- Relating to **cybercrime**, in Europe, the the most active operations have been Lockbit3, Ragroup, Cactus, 8Base, Play, and Qilin, while the most targeted sectors have been manufacturing, retail, technology, hospitality, and healthcare.
- Regarding **disruptive** activity, in late March over 1.600 planes experienced GPS interference over the Baltic Sea region. By mid March, cut submarine cables caused web outages across Africa, with 13 countries affected.
- About **information operations**, the US Treasury sanctioned individuals and companies based in Russia for their roles in a disinformation campaign. These entities allegedly crafted websites mimicking legitimate European government and media sites to spread pro-Russia disinformation.
- We noticed significant **data exposure and leaks** incidents in the technology (including artificial intelligence), military, telecommunications, public administration, and healthcare sectors. They were due to cybercriminal operations or accidental.

- On the **hacktivism** front, the pro-Russia self-claimed hacktivist group Noname057(16) launched DDoS attacks in several countries, and described the campaign as a “tour” of EU countries they consider anti-Russia.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in March 2024.

Europe

Cyber policy and law enforcement

Council and Parliament agree to strengthen cybersecurity capacities in the EU
On March 6, the Council and the European Parliament reached a provisional agreement on the Cyber Solidarity Act to enhance EU cyber resilience and cooperation. The act aims to improve threat detection, protect critical entities like hospitals, and strengthen EU solidarity and crisis management. It establishes a cybersecurity alert system through national and cross-border hubs for effective information sharing and threat response, enhance digital security across the EU for all citizens and businesses. `regulation`

Latvia’s Cabinet of Ministers approves draft national cyber security law
On March 19, Latvia’s Cabinet approved the National Cyber Security Law draft to enhance cyber capabilities and align with the EU’s NIS2 Directive. This introduces a National Cyber Security Center for supervising cybersecurity, policy development, and serving as the domestic cyber issues contact point. Essential service providers must register by April 1, 2025, and appoint a cybersecurity manager by July 1, 2025. The law mandates minimum cybersecurity standards, incident reporting, and risk management plans. `regulation`

US FTC fines two Cyprus companies for deceptive antivirus software
On March 14, the US FTC fined Restoro and Reimage, two Cyprus-based tech companies, 26 million US dollars for misleading customers with fake antivirus software. The companies used false Microsoft Windows alerts to convince users their systems were infected and sold unnecessary software for 27 to 58 US dollars, exploiting particularly older customers. Post-purchase, the companies would further deceive customers into buying more services by claiming additional non-existent issues, costing hundreds more. `sanction`

NCSC-UK releases guidance on cloud-hosted SCADA systems
On March 18, NCSC-UK has published guidance on securing cloud-based Supervisory Control and Data Acquisition (SCADA) systems. Recognising the shift from traditionally air-gapped operational technology to cloud-connected solutions, the guidance emphasises the need for robust authentication measures, such as single sign-on (SSO) or role-based access control (RBAC), alongside cloud-native key management services. It highlights the benefits of cloud migrations for centralising remote and privileged access management of SCADA systems. `guidance`

Germany takes down largest German-speaking cybercrime market
On March 1, the Düsseldorf Police in Germany announced having seized Crimemarket, the largest German-speaking illicit trading platform, arresting six individuals, including one operator. With over 180.000 users, Crimemarket facilitated the trade of illegal drugs, narcotics, and cybercrime services, along with hosting tutorials for criminal activities. The operation involved executing 102 search warrants across Germany on February 29. `take down`

German police shut down Nemesis darknet marketplace
On March 21, the German authorities dismantled the infrastructure of the illicit darknet marketplace Nemesis, removing its online presence. In a creative twist, visitors to the site were

met with a red banner and an animated spaceship, styled after the 1990s video game Nemesis, that destroys the marketplace's logo and then displays a QR code linking to the German federal police website. `take down`

Cyberespionage

Russia-linked APT29 targets German political parties
On March 22, cybersecurity firm Mandiant reported that, in late February, the Russia-linked APT29 used a new backdoor variant publicly tracked as Wineloader to target German political parties with a CDU-themed lure. Mandiant said this is the first time they have seen this APT29 cluster target political parties, indicating a possible area of emerging operational focus beyond the typical targeting of diplomatic missions. `russian threat actor`

Russia-linked APT28 phishing continues throughout the first quarter in 2024
On March 11, IBM-X reported that APT28 sent spearphishing e-mails throughout the first quarter of 2024. The e-mails targeted entities in the European governmental and NGO sector. Lures featured a mixture of internal and publicly available documents, among others, a Polish entity was impersonated as part of the campaign. The campaign attempted to install Macepie, a new backdoor, on its target's IT environment. `russian threat actor`

Chinese threat actor Earth Krahang targets European countries too
On March 18, Trend Micro reported on an APT campaign, linked to the China-nexus Earth Krahang group, targeting government entities and sectors across Southeast Asia, Europe, America, and Africa. Tactics involve exploiting vulnerabilities, abusing government infrastructure, and establishing VPNs for network access, with a focus on government, education, and telecommunications. Earth Krahang employs advanced post-exploitation techniques, indicating a sophisticated and wide-reaching cyberespionage effort. `chinese threat actor`

China-linked APT31 targeted UK's Parliament and stole electoral data in 2021
On March 25, the UK's National Cyber Security Center (NCSC-UK) reported that APT31 targeted UK parliamentarians' e-mails in 2021. The MPs involved were critical of Chinese policies. The report also points to the link between a Chinese state-affiliated actor and the compromise of computer systems of the UK Electoral Commission between 2021 and 2022. NCSC-UK assesses it is highly likely the attackers accessed and exfiltrated e-mail data, and data from the Electoral Register during this time. `chinese threat actor`

Finland associates 2020-2021 parliament hack to China-linked APT31
On March 26, the Finnish police confirmed that the APT31 was behind a breach of the country's parliament disclosed in March 2021. US authorities and other sources associate APT31 with the Chinese Ministry of State Security (MSS). `chinese threat actor`

Information operations

Russian-backed network allegedly paid European politicians
On March 29, BBC reported that authorities in several countries claimed to have broken up a Russian-backed "propaganda" network accused of spreading anti-Ukraine stories and allegedly paying undisclosed European politicians. The network reportedly used the Voice of Europe website as a conduit for payments to politicians, with investigations suggesting attempts to influence upcoming elections for the European Parliament. `russian threat actor`

Disruption

GPS jamming in Eastern Europe
Between March 24 and 26, over 1.600 planes experienced GPS interference over the Baltic Sea region. News reports associate the jamming activity to Russian activities. The interference involved jamming and spoofing which disrupted pilots' navigational data. It mainly occurred in Polish airspace but was also noted in Germany, Denmark, Sweden, Latvia, and Lithuania. `jamming`

Data exposure and leaks

German high-level military discussion leaked by Russia
On March 2, the German Federal Ministry of Defence confirmed that a video conference discussion among high-level German Air Officers was leaked by Russia. The conversation allegedly involved discussions about using Taurus cruise missiles to target the Crimea Bridge, which Russia perceives as evidence of the West's hybrid war against them. However, the complete authenticity of the leaked conversation is yet to be verified. `military`

65.000 government documents leaked in Switzerland
Xplain, a Swiss tech firm, fell victim to Play ransomware on May 23, 2023. The attackers purportedly accessed confidential data, later releasing it on the darknet. On March 7, 2024, the Swiss government confirmed the leak of 65.000 documents, mostly affecting units of the Federal Department of Justice and Police. Among them, 5.000 contained sensitive personal and classified data, while a smaller subset included IT system details and passwords. `technology`

Cyberattack on France Travail exposes millions of personal data records
On March 13, France Travail announced that it had been the victim of a cyberattack involving personal data of potentially 43 million people. The exposed data includes names, birth dates, social security numbers, and contact details, but passwords and bank details are not at risk. The attack occurred between February 6 and March 5. `public administration`

Cybercriminals threaten to leak NHS Scotland data
In late March, INC Ransom threatened to release 3TB of NHS Scotland's stolen data unless a ransom is paid, with the cybercriminals already sharing medical details and indicating an imminent leak. The cyberattack affecting NHS Dumfries and Galloway, a regional health board in Scotland, resulted in the unauthorised access and publication of clinical data, prompting collaboration between various entities to address the breach and support affected individuals. `health`

Hacktivism

Pro-Russia supposed hacktivist Noname057(16) claims responsibility for DDoS attacks against European countries
From March 2 to 7, the pro-Russia supposed hacktivist group NoName057(16) targeted websites in Belgium, Sweden, Czechia, Poland, and Denmark with DDoS attacks, using their DDoSia toolkit. The attacks hit government, financial, transportation, logistics, and aviation sectors. Motivations cited included political tensions in Moldova and farmers' protests in Poland. NoName057(16) described the campaign as a "tour" of EU countries they consider anti-Russia, affecting various essential services. `russian threat actor`

Anonymous Sudan target French government entities with DDoS
On March 10, French public services faced a DDoS attack, lasting until March 12, and targeting

an interministerial network infrastructure called RIE. Though attribution is unconfirmed, Anonymous Sudan, a pro-Russia supposed hacktivist group, claimed responsibility. The techniques used resemble those of Anonymous Sudan, Noname057(16), and others from the past two years. `russian threat actor` `public administration`

NoName targets Romanian government and finance sector
From March 14 to 19, the pro-Russia supposed hacktivist group Noname057(16) conducted a DDoS campaign against at least 25 websites associated with Romanian government and financial entities. The threat actor conducted the campaign in retaliation for the expansion of a multinational military base in Romania. At least one victim organisation confirmed the attacks. `russian threat actor` `finance` `public administration`

Pro-Russia supposed hacktivists claim DDoS attack on Luxembourg government sites
On March 21, Luxembourg governmental websites experienced downtime. The High Commission for National Protection, the governmental body responsible for coordinating national security and crisis management, confirmed the attack was a DDOS, affecting several state-run websites. The attack, claimed by pro-Russia supposed hacktivists on social media posts, was allegedly in retaliation for Luxembourg's involvement in ammunition purchases for Ukraine. `russian threat actor` `public administration`

World

Cyber policy and law enforcement

Predator spyware operators sanctioned in the United States
On March 6, the US sanctioned two individuals, and five entities connected to the development and dissemination of Predator spyware, created by the Intellexa consortium. Predator has been implicated in global operations targeting a wide range of individuals including government officials, journalists, politicians, activists, policy experts, and technology executives, contributing to human rights abuses and facilitating state-sponsored cyberespionage activities. `sanction` `psoa`

US levels new sanctions over Russian disinformation campaign
On March 20, the US Treasury announced sanctions against two individuals and companies, Social Design Agency and Company Group Structura LLC, based in Russia for their roles in a disinformation campaign. These entities allegedly crafted websites mimicking legitimate European government and media sites to spread Russian government disinformation. `sanction` `russian threat actor`

APT31 affiliation: US indicts Chinese firm and seven individuals for cyber intrusions
On March 25, the US Department of Justice unsealed an indictment against a Chinese firm and seven individuals associated with APT31 for cyber intrusions targeting US entities. The charges highlight the group's involvement in state-sponsored cyber operations, emphasising the persistent threat posed by nation-state actors. `indictment` `chinese threat actor`

Five Eyes cybersecurity agencies release Joint Fact Sheet for Leaders on Volt Typhoon
On March 19, Five Eyes cybersecurity agencies from Australia, Canada, the UK, New Zealand, and the US issued on Chinese state-sponsored Volt Typhoon cyber activity. In February, they warned that Chinese threat actors had infiltrated US critical infrastructure, maintaining access for up to five years. Volt Typhoon's unique targets and tactics aim to access operational technology assets within networks. `warning` `chinese threat actor`

Japan warns of DPRK IT workers seeking employment at Japanese companies
On March 26, the Japanese government issued an alert warning that North Korean IT workers are seeking employment with Japanese companies. This follows the March 7 report from the UN Security Council Panel of Experts report on DPRK activities that described how numerous North Korean nationals were working overseas to fund the country's nuclear and missile development programs. `warning` `north korean threat actor`

Canadian government discloses TikTok review over national security concerns
On March 14, the Canadian government announced a review of TikTok, started in September 2023, over national security worries related to its growth plans. This review, kept confidential under the Investment Canada Act, aligns with new policies addressing the threat of digital media manipulation by "hostile state-sponsored" actors. While details remain scarce, TikTok is cooperating with the ongoing scrutiny influenced by concerns over information manipulation and disinformation. `policy`

US Secure by Design Alert urges technology companies to conduct SQL injection code reviews
On March 25, US CISA and FBI issued a Secure by Design Alert. In the alert, they urge senior executives at technology manufacturers to mount a formal review of their code to determine its susceptibility to SQL injection compromises and encourage all technology customers to ask their vendors whether they have conducted such a review. `policy`

Microsoft announces deprecation of 1024-bit RSA keys in Windows
Microsoft will deprecate RSA keys under 2048 bits in Windows TLS, enhancing security. The shift from 1024-bit keys, which are less secure, to 2048-bit keys, increases protection significantly, with the latter considered safe until 2030. RSA keys, crucial for server authentication and data encryption, ensure communication integrity. The exact timeline for this deprecation is not detailed but will likely follow the pattern of prior updates, including a grace period. `policy`

UN General Assembly adopts AI resolution
On March 21, the United Nations General Assembly adopted an AI resolution aimed at safeguarding against potential AI-posed threats to human rights while allowing for technological advancements. `artificial intelligence`

US Congress members introduce bill to label deepfakes
On March 21, US Congress members introduced a bill to protect consumers from deceptive AI to the US House of Representatives. The bill highlights the need to label online content generated through AI to inform consumers by who and how the content was produced. `artificial intelligence`

Cyberespionage

Russia-linked ITG05 conducts worldwide phishing campaigns
According to IBM X-Force, a Russia-linked threat actor dubbed ITG05 has been engaging in global phishing campaigns since March, mimicking documents from governments and NGOs with a focus on finance, infrastructure, and cybersecurity. Since November 2023, they've started using new tactics like the "search-ms" URI handler for distributing malware through WebDAV servers, and introduced Masepie and Oceanmap backdoors. `russian threat actor`

Initial access broker shows indications of exploiting n-days for Chinese Ministry of State Security
On March 21, Mandiant publicly reported that UNC5174 (aka Uteus) has shown indications of acting as a contractor for China's Ministry of State Security (MSS) as an initial access broker. Mandiant reports that UNC5174 has been observed attempting to sell access to US defence contractor appliances, UK government entities, and institutions in Asia in late 2023 following CVE-2023-46747 exploitation. In February 2024, UNC5174 was observed exploiting a

ConnectWise ScreenConnect vulnerability (CVE-2024-1709) to compromise hundreds of institutions primarily in the US and Canada. `chinese threat actor`

New Zealand says APT40 targeted its parliament in 2021
On March 26, the New Zealand government said it had raised concerns with the Chinese government about its involvement in a state-sponsored cyber hack on New Zealand's parliament in 2021, which was uncovered by the country's intelligence services. The attack is being associated with APT40. `chinese threat actor`

Chinese threat actors target ASEAN entities in cyberespionage campaigns
On March 27, Palo Alto Networks reported that two Chinese advanced persistent threat (APT) groups have been conducting cyberespionage campaigns targeting ASEAN-affiliated entities throughout 2024, with one group, Stately Taurus, leveraging the ASEAN-Australia Special Summit for its activities, while another Chinese APT group remained unnamed but was found targeting ASEAN-affiliated entities as well. `chinese threat actor`

Iran-linked Curious Serpens' FalseFont backdoor
On March 21, Palo Alto Networks reported about a recently discovered backdoor, dubbed FalseFont, used by an Iranian-linked threat actor tracked as Curious Serpens. Curious Serpens (aka Peach Sandstorm, APT33, Elfin) is a cyberespionage group that has previously targeted the aerospace and energy sectors. In recent activities, the threat actors mimic legitimate human resources software, using a fake job recruitment process to trick victims into installing the backdoor. `iran threat actor`

North Korea-linked Kimsuky exploiting ScreenConnect vulnerabilities to drop new ToddleShark malware
On March 4, researchers at Kroll reported that the North Korean APT group Kimsuky is leveraging vulnerabilities in ScreenConnect (CVE-2024-1708 and CVE-2024-1709) to disseminate a new espionage-focused malware called ToddleShark. This malware, believed to be an iteration of their previous tools like BabyShark and ReconShark, targets governmental organisations, research centres, universities, and think tanks across the US, Europe, and Asia. `north korean threat actor`

New Predator spyware infrastructure targets civil society globally
On March 1, Recorded Future's Insikt Group reported new deployments of Predator, a mobile spyware, in eleven countries, notably for counterterrorism and law enforcement. Despite such claims, it's often used against civil society, journalists, politicians and activists without identifying specific targets. Countries affected include Angola, Armenia, Botswana, Egypt, Indonesia, Kazakhstan, Mongolia, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago. `psoa`

Google reports surge in zero-day exploits tied to spyware vendors
On March 27, Google's Threat Analysis Group and Mandiant reported a surge in zero-day vulnerabilities exploited in 2023, with spyware vendors implicated in half of these attacks, notably targeting Google products and Android devices. Commercial surveillance vendors were responsible for 75 procent of known zero-day exploits on these platforms and approximately half of all zero-day exploits in 2023, prompting Google to recommend enhanced security measures for high-risk users and sanctions against spyware operators by regulatory authorities. `psoa`

E-mails breached at the IMF
On March 15, the International Monetary Fund (IMF) revealed a cybersecurity incident involving 11 e-mail accounts, detected in February 2024. Apart from the unauthorised access to the e-mail accounts, no further system or resource breaches have been indicated. The affected accounts were on Microsoft 365. `unattributed threat actor`

Cybercrime

Magnet Goblin threat actor use 1-day flaws to drop custom Linux malware
On March 8, CheckPoint reported on Magnet Goblin, a cybercrime actor exploiting 1-day vulnerabilities in internet-facing services since January 2022. Targeting services like Ivanti VPN, Magento, and Qlik Sense, they rapidly adapt their methods. Their recent January 2024 campaign against Ivanti unveiled a new Linux NerbianRAT malware and the JavaScript credential thief Warpwire. `1-day exploitation`

Top.gg Discord bot source code poisoned
On March 25, Checkmarx Research team detailed how the Top.gg Discord bot community with over 170.000 members had been impacted by a supply-chain attack. The attack aimed to infect developers with malware that steals sensitive information through the poisoning of source code. `supply-chain attack`

Data exposure and leaks

12,8 million GitHub secrets on Github in 2023
On March 11, GitGuardian reported that in 2023, GitHub users accidentally exposed 12,8 million sensitive secrets in over 3 million public repositories, with most secrets still valid after five days. Despite 1.8 million alerts to users, only 1,8% acted swiftly to secure the data. The leaks included passwords, API keys, and TLS/SSL certificates. `technology`

Documentation startup Mintlify discloses data breach exposing customer GitHub tokens
On March 13, Mintlify, a company proposing AI-powered solutions to help developers produce code documentation, reported a security incident involving the compromise of 91 GitHub tokens. An e-mail alerted them to endpoint security concerns, leading to the discovery of unauthorised access by an unrecognised device, indicating possession of private admin tokens. Actions taken include revoking GitHub tokens, rotating admin tokens, and enhancing security. `artificial intelligence`

Threat actors leaked 70 million records allegedly stolen from AT&T
In mid-March, researchers at vx-underground reported that over 70 million records from an unspecified AT&T department were stolen in 2021 and surfaced on the Breached hacking forum in March 2024. ShinyHunters, a cybercrime group, initially claimed in August 2021 to have accessed a database with data on 70 million US AT&T customers. However, AT&T has disputed this claim. `telecommunications`

Misconfigured Firebase instances leaked 19 million plaintext passwords
In mid-March, researchers discovered 19 million plaintext passwords and over 125 million sensitive records exposed online due to misconfigured Firebase instances. Firebase is Google platform for hosting databases, cloud computing, and app development. Scanning over five million domains, the researchers identified 916 websites with inadequate security. The exposed data included e-mails, passwords, phone numbers, and bank details. Despite efforts to alert affected companies, with 842 e-mails sent, only 1% responded, yet a quarter corrected their Firebase security settings. `technology`

Data breach exposes 20 million Cutout.Pro user records on underground forum
On February 29, Bleeping Computer reported that the AI-powered visual design platform Cutout.Pro suffered a data breach exposing the personal details of 20 million users, including e-mail addresses, passwords, and other sensitive information. `artificial intelligence`

Disruption

Cut submarine cables cause web outages across Africa

On March 14, 13 African countries were affected by internet outages as a result of damaged fibre-optic cables in the Red Sea. According to a press release from the Nigerian Communications Commission the cuts occurred somewhere in Cote d'Ivoire and Senegal, with an attendant disruption in Portugal. Microsoft said that multiple cables on the West African coast were disrupted, but the source of the cable damage is unknown.

Significant vulnerabilities

Vulnerabilities in JetBrains TeamCity

On March 4, JetBrains released a fix for two vulnerabilities affecting JetBrains TeamCity CI/CD server. Both vulnerabilities are authentication bypass vulnerabilities. If exploited, the most severe vulnerability allows for a complete compromise of a vulnerable TeamCity server by a remote unauthenticated attacker, including unauthenticated RCE. See CERT-EU's SA 2024-23.

Vulnerabilities in VMware Products

On March 5, 2024, VMware released fixes for four vulnerabilities affecting several VMware products. The most serious bugs could allow a malicious actor with local admin privileges on a virtual machine to execute code as the virtual machine's VMX process running on the host. It is recommended upgrading affected software as soon as possible. See CERT-EU's SA 2024-24.

Zero-Day Vulnerabilities in Apple Products

On March 5, 2024, Apple released new product versions providing fixes for several vulnerabilities affecting iOS and iPadOS, among which 2 zero-day vulnerabilities already exploited in the wild. It is recommended updating as soon as possible. See CERT-EU's SA 2024-25.

Vulnerabilities in GitLab

On March 6, 2024, GitLab released a security advisory addressing several vulnerabilities that could lead to a security policy bypass and a breach of data confidentiality. See CERT-EU's SA 2024-26.

VCritical Vulnerabilities in Microsoft Products

On March 12, 2024, Microsoft addressed 60 vulnerabilities in its March 2024 Patch Tuesday update, including 18 remote code execution (RCE) vulnerabilities. See CERT-EU's SA 2024-27.

Vulnerabilities in Fortinet Products

On March 12, 2024, Fortinet released fixes for three vulnerabilities affecting some of their products. The vulnerabilities could allow an unauthenticated attacker to execute unauthorised code or commands via specifically crafted requests. See CERT-EU's SA 2024-28.

Vulnerabilities in Atlassian Products

On March 19, 2024, Atlassian released a security advisory addressing 24 high and critical vulnerabilities, among which a critical severity vulnerability in Bamboo Data Center/Server and a high vulnerability in Confluence Data Center and Server. See CERT-EU's SA 2024-29.

Critical Vulnerabilities in Ivanti Products

On March 20, 2024, Ivanti released fixes for two critical vulnerabilities affecting Ivanti Standalone Sentry and Ivanti Neurons for ITSM. According to Ivanti, there is no evidence of these vulnerabilities being exploited in the wild. See CERT-EU's SA 2024-30.

High Severity Vulnerabilities in Cisco Products

On March 27, 2024, Cisco released security updates for fourteen (14) vulnerabilities affecting IOS, IOS XE and Cisco Access Point software. Six (6) high severity vulnerabilities with a CVSS

score of 8.6, could allow an unauthenticated, remote attacker to cause denial of service on an affected device. See CERT-EU's SA 2024-31.

Critical Vulnerability in XZ Utils
On March 29, several companies issued a warning regarding a backdoor found in the XZ Utils software. XZ Utils is a data compression software and may be present in Linux distributions. The malicious code may allow unauthorised access to affected systems. See CERT-EU's SA 2024-32.

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.