# Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16 - 31 March 2024

*Source: AP News*

*Date: 22 March 2024*

## The UN adopts a resolution backing efforts to ensure artificial intelligence is safe

"The General Assembly approved the first United Nations resolution on artificial intelligence Thursday, giving global support to an international effort to ensure the powerful new technology benefits all nations, respects human rights and is "safe, secure and trustworthy." The resolution, sponsored by the United States and co-sponsored by 123 countries, including China, was adopted by consensus with a bang of the gavel and without a vote, meaning it has the support of all 193 U.N. member nations." READ MORE

*Source: Lawfaremedia*

*Date: 26 March 2024*

## So Close, So Far: UN Committee Tasked With Cybercrime Convention Hits Snooze

"[…] At the core of the disagreements lies a question of balance: How can the UN convention achieve robust international cooperation in the fight against cybercrime while offering strong protection of fundamental freedoms? What is already a delicate balance for democratic states becomes a challenge at the global level when dealing with states that do not share the same level of human rights protection. The interest blocs during the negotiations were fairly straightforward: China and Russia, and a small constellation of states around them, would prefer broad criminalization that captures a wide range of cyber activity. At the other end, states more closely aligned with the Budapest Convention saw Russia's position as a thinly veiled attempt to use the UN convention to weaken fundamental principles of human rights." READ MORE

*Source: INTERPOL*

*Date: 18 March 2024*

## Disrupting a Grandoreiro malware operation

"Brazil and Spain use INTERPOL's cyber capabilities to connect the dots between investigations. In January this year, Brazilian authorities announced the arrest of five administrators behind a Grandoreiro banking trojan operation. Considered a major cybersecurity threat across Spanish-speaking countries since 2017, Grandoreiro malware is introduced through phishing emails impersonating recognized organizations such as courts or telecom and energy companies." READ MORE

*Source: Hackread*

*Date: 25 March 2024*

## International Sting Takes Down Major Dark Web Marketplace "Nemesis Market"

"Nemesis Market, a major darknet marketplace for illegal goods, shut down by joint international law enforcement action – Servers seized, €94,000 in crypto confiscated. Global effort disrupts dark web criminal activity. In a coordinated international effort, German authorities, working alongside law enforcement agencies from the United States and Lithuania, have successfully shut down the global darknet marketplace "Nemesis Market."" READ MORE

RELATED ARTICLE: CyberDaily, Nemesis Market dismantled by German law enforcement, 25 March 2024

*Source: European Commission*

*Date: 25 March 2024*

## Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act

"Today, the Commission has opened non-compliance investigations under the Digital Markets Act (DMA) into Alphabet's rules on steering in Google Play and self-preferencing on Google Search, Apple's rules on steering in the App Store and the choice screen for Safari and Meta's "pay or consent model".The Commission suspects that the measures put in place by these gatekeepers fall short of effective compliance of their obligations under the DMA." READ MORE

*Source: IWF*

*Date: 18 March 2024*

## Teenage boys targeted as hotline sees 'heartbreaking' increase in child 'sextortion' reports

"Child sexual extortion, or "sextortion" reports have rocketed eightfold in a year – with boys being deliberately targeted by online criminals. New data published today (March 18) by the Internet Watch Foundation (IWF) shows in 2023, IWF analysts confirmed 176 reports of sexual extortion that contained child sexual abuse material. This is more than eight times as many as the previous year, when 21 cases of sexual extortion were recorded. Boys are targeted most often in the reports received by the IWF (91%), with analysts frequently seeing evidence of boys being blackmailed by criminals looking to extort money. Three in five (60%) reports involved 16 and 17-year-olds.'' READ MORE

*Source: European Commission*

*Date: 26 March 2024*

## Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections

"Today, the Commission has published guidelines on recommended measures to Very Large Online Platforms and Search Engines to mitigate systemic risks online that may impact the integrity of elections, with specific guidance for the upcoming European Parliament elections in June. Under the Digital Services Act (DSA), designated services with more than 45 million active users in the EU have the obligation to mitigate the risks related to electoral processes, while safeguarding fundamental rights, including the right to freedom of expression. […] The guidelines represent best practices for mitigating risks related to electoral processes at this moment in time." READ MORE

RELATED ARTCILE: Politico, Europe wields new tech law to protect EU election, 26 March 2024

*Source: Info security magazine*

*Date: 18 March 2024*

## IMF Investigates Serious Cybersecurity Breach

"The International Monetary Fund (IMF) said it is investigating a cybersecurity breach which led to the compromise of several internal email accounts. The Washington-headquartered UN financial agency revealed in a brief statement on Friday that the incident was first detected on February 16. "A subsequent investigation, with the assistance of independent cybersecurity experts, determined the nature of the breach, and remediation actions were taken," it added." READ MORE

*Source: The Guardian*

*Date: 21 March 2024*

## Nearly 4,000 celebrities found to be victims of deepfake pornography

"More than 250 British celebrities are among the thousands of famous people who are victims of deepfake pornography, an investigation has found. A Channel 4 News analysis of the five most visited deepfake websites found almost 4,000 famous individuals were listed, of whom 255 were British. They include female actors, TV stars, musicians and YouTubers, who have not been named, whose faces were superimposed on to pornographic material using artificial intelligence. The investigation found that the five sites received 100m views in the space of three months.early 4,000 celebrities found to be victims of deepfake pornography." READ MORE

*Source: Emol Social Facts*

*Date: 30 March 2024*

## Aumento de los ciberataques en Chile en 2023: Lo que dicen las cifras, las formas más frecuentes y las consecuencias

"[…] De acuerdo con la empresa de seguridad informática israelí, Check Point, en marzo de este año, los intentos de ciberataques en Chile casi se cuadruplicaron en dos semanas, posicionando al país como el cuarto entre los cinco con más intentos de ataques en el mundo. Entre Mongolia, Nepal, Indonesia y Taiwán, Chile es el único país perteneciente al hemisferio occidental en el ranking." READ MORE

*Source: Forbes Peru*

*Date: 25 March 2024*

## El Perú sufrió 5.000 millones de intentos de ciberataques en 2023, reportó Fortinet

"El Perú recibió 5.000 millones de intentos de ciberataques en 2023, según datos de FortiGuard Labs, el laboratorio de análisis e inteligencia de amenazas de Fortinet. Si se compara la cifra con el año anterior (15.000 millones de intentos de ciberataques en el 2022), es bastante menor, pero eso no es necesariamente una buena noticia. Esta es una tendencia global, ya que se observa una menor cantidad de ataques masivos y un mayor volumen de explotaciones únicas y variantes nuevas de malware y ransomware que son mucho más dirigidos, señala FortiGuard Labs." READ MORE

*Source: Infobae*

*Date: 19 March 2024*

## Nueva modalidad de estafa en Colombia: por WhatsApp promueven falsas inversiones en criptomonedas

"En Colombia, una sofisticada forma de estafa denominada *pig butchering* comenzó a generar alarma entre las autoridades y especialistas en ciberseguridad. Esta modalidad, que ya ha provocado pérdidas millonarias en Estados Unidos, implica engaños a través de WhatsApp, prometiendo falsas inversiones en criptomonedas. La estafa consiste en establecer contacto con potenciales víctimas mediante aplicaciones de mensajería o redes sociales, simulando errores en el envío de mensajes para captar la atención." READ MORE

*Source: Primicias*

*Date: 24 March 2024*

## Fraudes impulsados por la Inteligencia Artificial aumentan en Ecuador y el mundo

"[…] Los casos de estafas relacionados con imágenes, videos o audios manipulados con técnicas de Inteligencia Artificial (conocidos como deepfakes) se han disparado entre 2022 y 2023 en países de todo el mundo. Lo dice un reciente informe de la empresa inglesa Sumsub, proveedora de verificación de identidad. Países de Latinoamérica, como Ecuador, también experimentan el fenómeno En la región, los casos de estafa con Inteligencia Artificial se incrementaron 411% en el último año." READ MORE

*Source: MPF Brasil*

*Date: 19 March 2024*

## Brasil: Supremo Tribunal Federal Suíço determina repatriação de US$ 16,3 milhões de contas vinculadas a Paulo Maluf

"[…] A decisão do Supremo Suíço foi proferida em 2 de fevereiro de 2024 e é fruto de relevante cooperação contra a corrupção e a lavagem de dinheiro nos âmbitos nacional e internacional. Ela foi obtida a partir de um pedido de cooperação apresentado pelo MPF, por meio da Secretaria de Cooperação Internacional, à Confederação Suíça. O trâmite foi feito via Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça (DRCI/Senajus/MJSP), com o objetivo de buscar informações financeiras, bloqueio e repatriação de valores depositados em contas bancárias ligadas a Maluf, decorrentes dos crimes pelos quais ele foi condenado pelo Supremo Tribunal Federal (STF) na Ação Penal nº 863." READ MORE

*Source: RFI*

*Date: 29 March 2024*

## Mali: l'économiste Étienne F. Sissoko sera jugé pour un livre dénonçant la «propagande» des autorités

"Arrêté lundi soir, Étienne Fabaka Sissoko a été présenté mercredi 27 mars au procureur du Pôle judiciaire anti-cybercriminalité. Il est notamment accusé d'« atteinte au crédit de l'État ». Sa défense dénonce un énième procès politique. « Atteinte au crédit de l'État », « injures », « propos et nouvelles fausses mensongèrement attribuées à des tiers, faites de mauvaise foi et de nature à troubler la paix publique » READ MORE

*Source: The Record*

*Date: 26 March 2024*

## Detained execs, a bold escape, and tax evasion charges: Nigeria takes aim at Binance

"In cryptocurrency and law enforcement circles, Tigran Gambaryan is a bit of a legend. As a special agent with the Internal Revenue Service he investigated financial crimes and he came to specialize in something a lot of agents, at least initially, didn't quite understand: the blockchain. […] Which is why this week — when Nigeria announced that it had charged Gambaryan, who now works for the cryptocurrency platform Binance, another of the company's executives and the company itself with tax evasion — it rocked the crypto world. Nigeria's Federal Inland Revenue Service said on Monday that Binance didn't file tax returns or pay value added or corporate tax." READ MORE

*Source: Africa Cybersecurity Magazine*

*Date: 26 March 2024*

## L'OCRC au Bénin appréhende quatre suspects de cybercrime à Parakou

“La lutte contre la cybercriminalité se poursuit au Bénin. Pour cause, l'Office central de répression de la cybercriminalité (OCRC) de Parakou a procédé mercredi 20 mars 2024 dernier à l'arrestation de quatre individus soupçonnés d'activités cybercriminelles. Les suspects ont été appréhendés dans le quartier de Kpérou Guéra, situé en périphérie du premier arrondissement de Parakou. D’après les informations des médias locaux, c’est suite à une alerte que les éléments de l'OCRC ont pu localiser ces derniers.” READ MORE

*Source: Africa Cybersecurity Magazine*

*Date: 27 March 2024*

## Civic Watch se mobilise contre la désinformation en ligne avant les élections au Cameroun

“Dans le contexte des élections à venir au Cameroun, Civic Watch, une association camerounaise de lutte contre la désinformation, intensifie ses efforts pour contrer les risques associés à la désinformation en ligne. Cette semaine du 27 au 28 mars, l'organisation tiendra une réunion cruciale pour discuter des stratégies visant à faire face à cette menace croissante et à promouvoir la vérification des faits en Afrique. Sous la bannière de la campagne defyhatenow, cette réunion rassemblera des experts du Kenya, d'Afrique du Sud et du Nigeria, […].” READ MORE

*Source: Japap*

*Date: 27 March 2024*

## Guinée Équatoriale: Analyse du Projet Loi Régulant l’Utilisation des Réseaux Sociaux et du Cyberespace

“[…] Si ce projet de loi est approuvé, les mineurs de moins de 14 ans ne pourront pas utiliser les réseaux sociaux sans consentement écrit de, leurs parents ou tuteurs. De plus, toutes les données et informations publiées sur ces plateformes devront avoir obtenu un consentement explicite au préalable. Il sera également interdit de publier des données, des informations, des fichiers, des photos ou des vidéos, d’autres personnes sans leur consentement écrit. Cela inclut également le téléchargement illégal de contenus protégés par le droit d’auteur et la création de faux profils.” READ MORE

*Source: The Record*

*Date: 20 March 2024*

## Hackers claim to have breached Israeli nuclear facility’s computer network

“An Iran-linked hacking group claims to have breached the computer network of a sensitive Israeli nuclear installation in an incident declared by the ‘Anonymous’ hackers as a protest against the war in Gaza. The hackers claim to have stolen and published thousands of documents — including PDFs, emails, and PowerPoint slides — from the Shimon Peres Negev Nuclear Research Center. […] While the documents that have been released potentially suggest the hackers were able to compromise an IT network connected to the facility, there is no evidence they have been able to breach its operational technology (OT) network.” READ MORE

*Source: Hackread*

*Date: 16 March 2024*

## Hackers Claim Accessing 740GB of Data from Viber Messaging App

“Pro-Palestinian hackers calling themselves “Handala Hack” claim to have accessed 740GB of data from the messaging app Viber, including source code – Viber denies the breach but is investigating – Users are advised to change passwords. […] In its Telegram post, Handala Hack alleged they stole over 740GB of data, including Viber’s source code. The group demands a ransom of 8 Bitcoin, or $583,000, for the stolen information. […] The company has denied any evidence of intrusion into its systems or data compromise but confirmed that it has already launched an investigation to verify if a security breach has occurred.” READ MORE

*Source: Reuters*

*Date: 31 March 2024*

## India rescuing citizens forced into cyber fraud schemes in Cambodia

“The Indian government said it was rescuing its citizens who were lured into employment in Cambodia and were being forced to participate in cyber fraud schemes. The Indian embassy in Cambodia is working with Cambodian authorities and has rescued and repatriated about 250 Indians, including 75 in the last three months, India's Ministry of External Affairs spokesperson Randhir Jaiswal said in a statement on Saturday. Jaiswal was responding to Indian news reports that stated more than 5,000 Indians are trapped in Cambodia and being forced to carry out cyber frauds on people back home.” READ MORE

*Source: Ukranews*

*Date: 18 March 2024*

## 268 telecom scam suspects handed over to China from Laos

“A total of 268 suspects involved in cross-border telecom frauds affecting Chinese citizens were returned from Laos to Chinese police custody, the Ministry of Public Security announced. The suspects, including eight who served as the crimes' funding source and 54 criminal ring heads and core members, have been implicated in over 1,570 relevant cases in multiple localities in China, the ministry said in a statement.” READ MORE

*Source: BitDefender*

*Date: 19 March 2024*

## Hackers demand ransom from New Zealanders whose data was allegedly stolen in a data breach at local media firm

“MediaWorks, a leading New Zealand radio, outdoor advertising, and interactive media company, is investigating a data breach that may have exposed the personal information of over 2.5 million people. Although the company has yet to confirm the incident, hackers are actively trying to exploit the allegedly stolen data by directly contacting victims with demands to make payments. “On Friday evening (15 March), we became aware of claims that MediaWorks had been subject to a cyber security incident,” the company said. “The claims relate to data from website competition entries. Last night, all current competition entries were moved to a new secure database.”” READ MORE

*Source: DW*

*Date: 22 March 2024*

## Russian hackers targeting German politicians

"Russian hackers have targeted several German political parties to steal data, German news magazine Der Spiegel reported on Friday. The magazine cited an analysis from the US security firm Mandiant, which is subsidiary of Google owner Alphabet, as well as an alert by German security authorities. Mandiant said that the APT29 hacking group, which is also known as "Cozy Bear," tried to trick "key German political figures" into opening an email that contained a fake invitation to a dinner event hosted by the opposition conservative Christian Democratic Union (CDU) party. […] An alert from Germany's Federal Office for Information Security (BSI) said that cyber spies were attempting to build long-term access and extract data from German political parties." READ MORE

*Source: U.S. Department of the Treasury*

*Date: 25 March 2024*

## Treasury Designates Russian Companies Supporting Sanctions Evasion Through Virtual Asset Services and Technology Procurement

"Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned thirteen entities and two individuals for operating in the financial services and technology sectors of the Russian Federation economy including persons developing or offering services in virtual assets that enable the evasion of U.S. sanctions. Five entities were designated for being owned or controlled by OFAC-designated persons." READ MORE

*Source: Bleeping Computer*

*Date: 26 March 2024*

## Germany warns of 17K vulnerable Microsoft Exchange servers exposed online

"The German national cybersecurity authority warned on Tuesday that it found at least 17,000 Microsoft Exchange servers in Germany exposed online and vulnerable to one or more critical security vulnerabilities. According to the German Federal Office for Information Security (BSI), around 45,000 Microsoft Exchange servers in Germany have Outlook Web Access (OWA) enabled and are accessible from the Internet." READ MORE

*Source: Dutch News*

*Date: 20 March 2024*

## The Netherlands: New sex crime legislation treats online and offline equally

"New legislation which will make it a crime to intimidate people sexually in public places, including social media, and which will make it easier to prosecute rape cases, will come into effect on July 1, justice minister Dilan Yesilgöz said on Wednesday. The new legislation removes the need to prove the attacker used force in rape cases and removes rape from the statute of limitations, so cases can still be prosecuted, no matter how long ago they took place. The law also makes it a criminal offence to approach children online and have conversations of a sexual nature with them – a crime known as sexchatting." READ MORE

*Source: Le Monde*

*Date: 19 March 2024*

## France : Cyber-harcèlement contre Magali Berdah : des peines de prison allant de quatre à dix-huit mois pour les 28 prévenus

"Le tribunal correctionnel de Paris a condamné, mardi 19 mars, les 28 personnes jugées entre novembre et janvier pour le cyber-harcèlement en meute de l'agente d'influenceurs Magali Berdah à des peines allant de quatre à dix-huit mois de prison, assorties de sursis dans la moitié des cas. Il s'agit de la plus grande affaire de cyber-harcèlement jugée devant la justice française. […] La peine la plus sévère prononcée mardi atteint douze mois de prison ferme. Les prévenus – âgés de 20 à 49 ans et résidant dans toute la France – ont, par ailleurs, été condamnés à des amendes allant de 300 à 700 euros, et à suivre un stage de citoyenneté." READ MORE

*Source: CryptoNews*

*Date: 21 March 2024*

## UK Woman Found Guilty of Laundering $2.5B Bitcoin

"A British woman has been found guilty and convicted on Wednesday for laundering over $2.5 billion (£2 billion) worth of bitcoin for a Chinese fugitive. Jian Wen, a 42 year old British citizen has been found guilty for money laundering on behalf of a Chinese woman called Yadi Zhang. The jury found Wen guilty on one count of money laundering and couldn't reach a decision on two other charges. In an announcement, the Crown Prosecution Service said the sheer scale of the seized Bitcoin, the lack of any legitimate evidence for how it was acquired and its connection to a massive investment fraud in China, all indicated that it was criminal property." READ MORE

*Source: US Department of Justice*

*Date: 25 March 2024*

## Former Computer Privacy Consultant Convicted of Cyberstalking

"A federal jury convicted a former privacy consultant last week for a cyberstalking campaign in which he sent electronic messages and made social media posts threatening sexual assault and other violence against multiple victims. […] The jury convicted Garg of one count of conspiracy to engage in cyberstalking, three counts of cyberstalking in violation of a criminal order, and three counts of cyberstalking. He is scheduled to be sentenced on June 25 and faces a mandatory minimum of one year in prison and a maximum penalty of 35 years in prison." READ MORE

*Source: US Department of Justice*

*Date: 25 March 2024*

## Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians

"An indictment was unsealed today charging seven nationals of the People's Republic of China (PRC) with conspiracy to commit computer intrusions and conspiracy to commit wire fraud for their involvement in a PRC-based hacking group that spent approximately 14 years targeting U.S. and foreign critics, businesses, and political officials in furtherance of the PRC's economic espionage and foreign intelligence objectives." READ MORE

*Source: Reuters*

*Date: 26 March 2024*

## Florida's DeSantis signs law restricting social media for people under 16

"Florida Governor Ron DeSantis on Monday signed a bill that bans children aged under 14 from social media platforms and requires 14- and 15-year-olds to get parental consent, a measure supporters say will protect them from online risks to their mental health.The measure requires social media platforms to terminate the accounts of people under 14 and those of people under 16 who do not have parental consent. It requires them to use a third-party verification system to screen out those who are underage." READ MORE

*Source: US Department of the Treasury*

*Date: 22 March 2024*

## Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts

"Moscow employs an array of tools, including malign influence campaigns and illicit cyber activities, to undermine the interests of the United States and its allies and partners, including in Latin America, the Middle East, and Europe. Russia routinely uses its intelligence services, proxies, and influence tools in these efforts. Russia's influence actors have increasingly adapted their methods to hide their involvement by developing a vast ecosystem of Russian proxy websites, personas, and organizations which give the false appearance of being independent news sources.'' READ MORE

RELATED ARTICLE:

ChainAnalysis, OFAC Sanctions Russian Nationals, 20 March 2024

## Latest reports

- Resecurity, The Aviation And Aerospace Sectors Face Skyrocketing Cyber Threats, 16 March 2024
- National Cyber Security Centre UK, Operational Technology. Making sense of cyber security in OT environments, 18 March 2024
- Proofpoint, FBI's IC3 Report: Losses from Cybercrime Surpass $12.5 Billion—a New Record, 18 March 2024
- CISA, PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders, 19 March 2024
- Palo Alto Networks, Unit 42 Collaborative Research With Ukraine's Cyber Agency To Uncover the Smoke Loader Backdoor, 19 March 2024
- HelpNetSecurity, Lynis: Open-source security auditing tool, 19 March 2024
- TrendMicro, TeamCity Vulnerability Exploits Lead to Jasmin Ransomware, Other Malware Types, 19 March 2024
- Securelist, Threat landscape for industrial automation systems, 19 March 2024
- Proofpoint, The 2024 Data Loss Landscape Report Explores Carelessness and Other Common Causes of Data Loss, 19 March 2024
- Security Affair, New Acidpour wiper targets Linux x86 devices. Is it a Russia's weapon?, 19 March 2024
- Trusted Sec, From Error to Entry: Cracking the Code of Password-Spraying Tools, 19 March 2024
- Hackread, Cybercriminals Beta Test New Attack to Bypass AI Security, 19 March 2024
- Kaspersky, State of Stalkerware 2023 report, 20 March 2024
- Krebsonsecurity, The Not-so-True People-Search Network from China, 20 March 2024
- Council of Europe, European Committee of Social Rights publishes 2023 Findings and Conclusions on Children, Family and Migrants, 20 March 2024
- The Register, Stalkerware usage surging, despite data privacy concerns, 20 March 2024
- Cyberpeace Institute, Monitoring the Harm to Civilians in Armed Conflict, 20 March 2024
- Sucuri, Sign1 Malware: Analysis, Campaign History & Indicators of Compromise, 20 March 2024
- Eurojust, Digital Services Act: ensuring a safe and accountable online environment, 20 March 2024
- Trustwave, Trustwave SpiderLabs: Artificial Intelligence Playing a Prime Role in BEC and Phishing Attacks, 20 March 2024
- CISA, Understanding and Responding to Distributed Denial-Of-Service Attacks, 21 March 2024
- Mandiant, Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect, 21 March 2024
- Talos Intelligence blog, New details on TinyTurla's post-compromise activity reveal full kill chain, 21 March 2024
- ProofPoint, Security Brief: TA450 Uses Embedded Links in PDF Attachments in Latest Campaign, 21 March 2024
- ChainAnalysis, Asset Tokenization Explained: Benefits, Risks, and How It Can, 22 March 2024
- Council of Europe/Cybercrime Programme Office, Discussion paper: Freedom of Expression within the Context of Action on Cybercrime, Practical considerations, [EN], 22 March 2024

- Council of Europe/Cybercrime Programme Office: Document de travail : La liberté d'expression dans le cadre de la lutte contre la cybercriminalité, Considérations pratiques [FR], 22 March 2024
- Council of Europe/Cybercrime Programme Office: Documento de debate: La libertad de expresión en el contexto de las medidas en materia de ciberdelincuencia - Consideraciones prácticas [ES], 22 March 2024
- Mandiant, APT29 Uses WINELOADER to Target German Political Parties, 22 March 2024
- Resecurity, Cybercriminals Accelerate Online Scams During Ramadan And Eid Fitr, 22 March 2024
- SecurityWeek, New 'GoFetch' Apple CPU Attack Exposes Crypto Keys, 22 March 2024
- Bleeping Computer, Over 100 US and EU orgs targeted in StrelaStealer malware attacks, 24 March 2024
- CISA, Secure by Design Alert: Eliminating SQL Injection Vulnerabilities in Software, 25 March 2024
- MIPA Institute, Cybersecurity in Morocco: between achievements and challenges, 25 March 2024
- INHOPE, The future of the Universal Classification Scheme, 25 March 2024
- Computer Security Group, ZenHammer: Rowhammer Attacks on AMD Zen-based Platforms, 25 March 2024
- Lumen, The Darkside Of TheMoon, 26 March 2024
- Paul Ducklin, GoFetch: It's Performance versus Security all over again!, 26 March 2024

  Related: The Register, Stalkerware usage surging, despite data privacy concerns, 20 March 2024
- Krebsonsecurity, Recent 'MFA Bombing' Attacks Targeting Apple Users, 26 March 2024
- The CypherBrief, Preparing for a Digital Battlefield: National Security and Cryptocurrency, 26 March 2024
- Unit42, ASEAN Entities in the Spotlight: Chinese APT Group Targeting, 26 March 2024
- ENISA, Foresight Cybersecurity Threats For 2030 - Update 2024: Executive Summary, 27 March 2024
- Krebsonsecurity, Thread Hijacking: Phishes That Prey on Your Curiosity, 28 March 2024
- Cyble, Solana Drainer's Source Code Saga: Tracing Its Lineage to the Developers of MS Drainer, 28 March 2024
- Securonix, Analysis of New DEEP#GOSU Attack Campaign Likely Associated with North Korean Kimsuky Targeting Victims with Stealthy Malware, March 2024

## Upcoming events

- 1-2 April 2024, C-PROC, (in person), Introductory course for Supreme Court judges, Mauritius, GLACY-e and Octopus
- 2-3 April 2024, C-PROC, (in person), Workshop on cybercrime legislation, Seychelles, Octopus
- 3-5 April, C-PROC, (in person), Consultation workshop on the cybercrime bill with key stakeholders, Rwanda, GLACY-e
- 1-15 April 2024, C-PROC, *(online)*, Translation into Arabic and dissemination among project partners of the updated version of the Guide on Electronic Evidence, CyberSouth+
- 8-12 April 2024, C-PROC, (in person), Training Course on cybercrime and electronic evidence for prosecutors (Advanced course), Brazil, GLACY-e and Octopus
- 11-12 April 2024, C-PROC 10th anniversary (in person), Romania, all projects
- April 2024, C-PROC (online), Further development of the Cyberviolence resource, Octopus
- April 2024, C-PROC, (online), Further development of the Octopus platform, Octopus
- April 2024, C-PROC, (online), Further development of the CYBOX training platform, Octopus

The Cybercrime Digest appears bi-weekly. The news is selected by relevance to the current areas of interest to C-PROC and does not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

**www.coe.int/cybercrime**

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE