Cybercrime Digest

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

16-29 February 2024

Source: Europol

Date: 20 February 2024

Law enforcement disrupt world's biggest ransomware operation

"In a significant breakthrough in the fight against cybercrime, law enforcement from 10 countries have disrupted the criminal operation of the LockBit ransomware group at every level, severely damaging their capability and credibility. […] This international sweep follows a complex investigation led by the UK's National Crime Agency in the framework of an international taskforce known as 'Operation Cronos', coordinated at European level by Europol and Eurojust. This includes the takedown of 34 servers in the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States and the United Kingdom. In addition, two LockBit actors have been arrested in Poland and Ukraine at the request of the French judicial authorities. Three international arrest warrants and five indictments have also been issued by the French and U.S. judicial authorities. Authorities have frozen more than 200 cryptocurrency accounts linked to the criminal organisation, underscoring the commitment to disrupt the economic incentives driving ransomware attacks." READ MORE

RELATED ARTICLES:

Reuters, Lockbit cybercrime gang says it is back online following global police bust, 26 February 2024

US Department of Justice, U.S. and U.K. Disrupt LockBit Ransomware Variant, 20 February 2024

U.S. Department of the Treasury, United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group, 20 February 2024

Reuters, Ukraine arrests father-son duo in Lockbit cybercrime bust, 22 February 2024

Source: Cyper Peace Institute

Date: 21 February 2024

UN Cybercrime Convention: negotiators request more time as consensus remains elusive

"The concluding session of the Ad Hoc Committee (AHC) negotiating a new United Nations cybercrime convention took place in New York from 29 January to 9 February. While some progress on the Treaty has been made, it was not sufficient to reach a consensus. Member states agreed to "suspend" the meeting and reconvene at a later date. This procedural move enables delegations to extend the cybercrime deliberations under the same modalities whilst keeping the initial deadline to deliver the draft Convention to the UN General Assembly at its seventy-eighth session." READ MORE

RELATED ARTICLES:

Economic Times India, Relook parts of draft cybercrime treaty: Rights groups to UN panel, 27 February 2024

PhilStar, Negotiations on treaty vs cybercrime still ongoing, 26 February 2024

Source: Reuters

Date: 29 February 2024

UnitedHealth hackers say they stole 'millions' of records, then delete statement

"In a message posted to, and then quickly deleted from their darknet site, the hackers blamed for striking the UnitedHealth Group (UNH.N), opens new tab said on Wednesday they stole millions of sensitive records, including medical insurance and health data, from the company. In its claim of responsibility, the group known as "Blackcat" or "ALPHV" posted a statement to its site saying it had stolen 8 terabytes of data from UnitedHealth, according to screenshots of the posting shared online by cybersecurity researchers." READ MORE

RELATED ARTICLES:

CNBC, Outages from cyberattack at UnitedHealth's Change Healthcare extend to seventh day as pharmacies deploy workarounds, 27 February 2024

Fierce Healthcare, Optum confirms BlackCat cybercriminal group behind Change Healthcare attack, 29 February 2024

Source: Eurojust

Date: 27 February 2024

Full-scale action against EUR 2 billion money laundering network via Lithuanian financial institution

"Eurojust supports joint investigation team with operations in Italy, Latvia and Lithuania, also tackling EUR 15 million Italian public money fraud. Judicial and law enforcement authorities in Italy, Latvia and Lithuania have taken concerted action against a large-scale money laundering business, centring around a Lithuanian financial institution. Since 2017, an estimated EUR 2 billion has been laundered by two main suspects via a worldwide web of shell companies. The suspects, who now have been detained, offered money laundering online as a service to criminals. A third main suspect, leading another organised crime group (OCG), was arrested in the same operation for defrauding the Italian authorities of EUR 15 million in public funds. These funds were laundered via the same myriad web of enterprises, centred around the financial institution in Lithuania." READ MORE

Source: Eurojust

Date: 21 February 2024

Over 100 searches and four arrests in Latvia, Germany, France, Italy and Malta against financial institution involved in money laundering

"National authorities in Latvia, Germany, France, Italy and Malta have carried out over 100 searches in a large-scale operation against a Russian-Eurasian criminal network and a Maltese-based financial institution allegedly involved in money-laundering services. Four suspects were detained during an action day supported by Eurojust and Europol. Potential suspects and witnesses were also interviewed in Latvia, Germany, Estonia and Malta. During the actions, over 460 police officers were deployed to carry out the searches. Germany also deployed four officers to support the investigations and searches in Latvia and Malta. In addition to the arrests, various bank accounts and properties were seized." READ MORE

Source: European Parliament

Date: 15 February 2024

Child sexual abuse online: agreement on extending current rules until April 2026

"Parliament and Council teams have agreed to extend an exemption to EU e-Privacy rules allowing for the detection of child sexual abuse material online until 3 April 2026. On Thursday, negotiators from the European Parliament and the Council of the EU reached an agreement on a temporary extension to the current e-Privacy derogation that allows for the voluntary detection of child sexual abuse material (CSAM) online." READ MORE

Source: Reuters

Date: 20 February 2024

EU opens formal investigation into TikTok over possible online content breaches

"The European Union will investigate whether ByteDance's TikTok breached online content rules aimed at protecting children and ensuring transparent advertising, an official said on Monday, putting the social media platform at risk of a hefty fine. EU industry chief Thierry Breton said he took the decision after analysing the short video app's risk assessment report and its replies to requests for information, confirming a Reuters story." READ MORE

Source: Euronews

Date: 17 February 2024

Big Tech companies sign accord to combat AI-generated election disinformation

"Meta, OpenAI, TikTok, Microsoft, and Amazon were among the agreement's signatories at the Munich Security Conference. Elon Musk's X also signed up. Major technology companies signed a pact on Friday to voluntarily adopt "reasonable precautions" to prevent artificial intelligence (AI) tools from being used to disrupt democratic elections around the world. Executives from Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, and TikTok gathered at the Munich Security Conference to announce a new framework for how they respond to AI-generated deepfakes that deliberately trick voters. READ MORE

RELATED ARTICLE:

Microsoft, Technology industry to combat deceptive use of AI in 2024 elections, 16 February 2024

Source: IWF

Date: 29 February 2024

Pioneering chatbot reduces searches for illegal sexual images of children

"A major 18-month trial project has demonstrated a first-of-its-kind chatbot and warning message can reduce the number of online searches that may potentially be indicative of intent to find sexual images of children. A new report published today by the University of Tasmania has found people looking for sexual images of children on the internet were put off, and in some cases sought professional help to change their behaviour, following the intervention of a ground-breaking chatbot trialed on the Pornhub website in the UK. […] This is the first project of its kind to use chatbot technology to intervene when people use search terms that suggest an interest in finding sexual images of children. It then tries to help them stop, or not start, offending." READ MORE

Source: US immigration and customs enforcement

Date: 296February 2024

Hombre de Florida es condenado a 27 años en prisión por distribuir, recibir y poseer material de abuso sexual infantil

"Una investigación de la Oficina de Investigaciones de Seguridad Nacional (HSI, por sus siglas en inglés) de Tampa condujo a una sentencia de prisión de 27 años por distribuir, recibir y poseer material de abuso sexual infantil. También se le ordenó a Jesse James Bertetto —30 años, de Webster— a inscribirse como delincuente sexual y pagar $74,500 en restitución luego de que un jurado federal lo declarara culpable el 12 de abril de 2023. Según testimonios y pruebas presentadas en el juicio, en diciembre de 2020, Bertetto poseía material de abuso sexual infantil en su teléfono celular, incluyendo imágenes y videos de menores de 12 años." READ MORE

Source: Business Wire

Date: 20 February 2024

Une nouvelle étude menée par l'ONG finlandaise Protect Children révèle comment les délinquants utilisent les plateformes technologiques pour commettre des abus sexuels contre des enfants en ligne

"Une nouvelle étude historique dévoile des informations alarmantes sur les plateformes technologiques dont les délinquants se servent pour abuser sexuellement des enfants en ligne. L'étude, qui s'est penchée sur plus de 30 000 possesseurs de matériel pédopornographique (child sexual abuse material, CSAM), révèle des informations importantes pour lutter contre la prolifération des abus sexuels et l'exploitation des enfants en ligne. La recherche a permis de révéler que 40 % de ces délinquants ont tenté d'entrer en contact avec un enfant, et que parmi ces derniers, 70 % ont initié ce contact en ligne, principalement via les réseaux sociaux, les jeux en ligne ou les plateformes de messagerie (Instagram, Facebook et Discord étant les plateformes de médias sociaux les plus exploitées." READ MORE

Source: Senado Noticias

Date: 21 February 2024

Brazil: CCJ aprova projeto para proteger crianças e adolescentes em ambientes digitais

"A Comissão de Constituição e Justiça (CCJ) aprovou nesta quarta-feira (21) o projeto de lei (PL) 2.628/2022, que busca proteger crianças e adolescentes em ambientes digitais. O projeto do senador Alessandro Vieira (MDB-SE) foi aprovado na forma do substitutivo apresentado pelo relator, o senador Jorge Kajuru (PSB-GO). Os senadores aprovaram um requerimento de urgência para a votação da matéria, que segue para a Comissão de Ciência e Tecnologia (CCT). O projeto prevê regras para redes sociais, aplicativos, sites, jogos eletrônicos, softwares, produtos e serviços virtuais — como a criação de mecanismos para verificar a idade dos usuários. O PL 2.628/2022 também impõe supervisão do uso da internet pelos responsáveis e obriga provedores de internet e fornecedores de produtos a criar sistemas de notificação de abuso sexual e oferecer configurações mais eficientes para a privacidade e a proteção de dados pessoais. " READ MORE

Source: Presidencia Republica Dominicana

Date: 28 February 2024

República Dominicana lidera el Grupo de Trabajo de Medidas de Fomento de la Confianza en el Ciberespacio de la OEA

"[…] La responsabilidad recae sobre el Centro Nacional de Ciberseguridad (CNCS), representado por Carlos Leonardo, director de Equipo de Respuesta a Incidentes Cibernéticos (CSIRT-RD) y del Ministerio de Relaciones Exteriores (Mirex), representado por Claudio Peguero, embajador de la República Dominicana para Asuntos Cibernéticos, quienes fungirán como puntos de contacto del Grupo de Trabajo de las MFC de la OEA. La escogencia se produjo este 27 de febrero, Día de la Independencia Nacional." READ MORE

Source: CoIntelegraph

Date: 21 February 2024

Se intensifican ataques de ransomware del Grupo Medusa en LATAM

"El grupo de cibercriminales Medusa ha incrementado sus ataques en latinoamérica, según revela una investigación de UNIT 42, la Unidad de Investigación y Amenazas de Palo Alto Networks. Especializado en el secuestro y encriptación de datos de organizaciones y empresas que utilizan Windows, Medusa ha intensificado sus tácticas de multiextorsión, haciendo uso del ransomware homónimo "Medusa"." READ MORE

Source: Africa Cyber Security

Date: 16 February 2024

Wave Digital Finance et la Police Judiciaire s'unissent pour lutter contre les activités illicites financières en ligne au Sénégal

"Wave digital finance et la Police judiciaire sénégalaise ont annoncé leur union mercredi 14 février 2024 lors de la cérémonie d'ouverture d'un atelier afin de lutter contre le blanchiment de capitaux, le financement du terrorisme et d'autres activités illicites. […] D'après les précisions du Directeur Idrissa CISSE, les unités d'enquêtes sont actuellement confrontées à des affaires complexes, d'où la nécessité pour tous les acteurs impliqués d'interagir et de partager leurs expériences pour détecter, identifier et traquer les cybercriminels où qu'ils se trouvent." READ MORE

Source: Business News

Date: 22 February 2024

Tunisie: Pourquoi faut-il réviser le décret 54 ?

"Le fameux décret liberticide 54 et son article 24 ne cessent de susciter la polémique. Le texte n'a fait que cumuler les critiques à un tel point que même les députés supposés soutenir le régime en place proposent une révision du décret. Avons-nous vraiment besoin de nous expliquer au sujet de ce triste texte ? Malheureusement oui, et voici les principales raisons justifiant l'amendement du décret." READ MORE

RELATED ARTICLE:

Kapitalis, Tunisie, liberté de la presse: initiative législative pour amender le décret-loi 54, 22 February 2024

Source: Africa Cyber Security Magazine

Date: 16 February 2024

La PLCC met fin à une tentative de chantage amoureux orchestrée par deux cybercriminels en Côte d'Ivoire

"La Plateforme de lutte contre la cybercriminalité (PLCC) a mis fin le 16 février 2024 dernier à une tentative de chantage orchestrée par deux individus, BMO et son complice SA, sur fond de vengeance amoureuse. L'affaire a débuté lorsque AD, une jeune femme blessée par une rupture avec son ex-petit ami, a engagé les services de ces cybercriminels pour ternir l'honneur de son ancien compagnon, YPA. […] À l'issue des investigations, les résultats ont permis de remonter jusqu'aux auteurs, BMO et SA, qui ont avoué leur implication dans cette tentative de chantage." READ MORE

Source: IPI-International Press Institute

Date: 19 February 2024

Nigeria: Journalists targeted again under cybercrime law

"The IPI global network calls on the authorities in Kwara State, Nigeria to stop using Nigeria's Cybercrimes Act and the penal code to target journalists and undermine media freedom. Earlier this month, on February 6, four journalists from the online news site Informant247 – Adisa-Jaji Azeez, Salihu Ayatullahi, Salihu Shola Taofeek, and Abdulrahman Taye Damilola – were recently arrested, detained, and charged with conspiracy, cyberstalking, and defamation." READ MORE

Source: US Department of Justice

Date: 21 February 2024

Prominent Ghanaian "Influencer" Pleads Guilty to Receiving Fraud Proceeds From Romance Scams

"From at least in or about 2013 through in or about 2019, MONTRAGE was a member of a criminal enterprise (the "Enterprise") based in West Africa that committed a series of frauds against individuals and businesses in the U.S., including romance scams. […] MONTRAGE is a Ghanaian public figure who rose to fame as an influencer through her Instagram profile under the username "Hajia4Reall," which at one point had approximately 3.4 million Instagram followers and was among the top 10 profiles with the most followers in Ghana." READ MORE

Source: Al Jazeera

Date: 19 February 2024

X faces restrictions in Pakistan amid protests over alleged vote rigging

"Social media platform X, formerly known as Twitter, continues to remain inaccessible to users in Pakistan after internet watchdog groups started to report outages on Saturday. NetBlocks, an organisation that monitors accessibility issues on the internet, On February 17 confirmed that a "national-scale disruption" has hit X in Pakistan in the aftermath of widespread protests in the country triggered by the alleged vote rigging in general elections. Government officials, however, have refused to acknowledge any such restriction." READ MORE

Source: Reuters

Date: 26 February 2024

China to increase protections against hacking for key industries

"China's ministry of industry and information technology (MIIT) unveiled a plan on Monday that aims to improve data security in China's industrial sector and effectively contain "major risks" by the end of 2026. The plan comes at a time when China and the United States both frequently accuse each other of cyberattacks and industrial espionage. Reuters reported last year that Chinese government entities and state-owned enterprises were accelerating efforts to replace Western-made hardware and software with domestic alternatives, partly due to fears of hacking from foreign adversaries." READ MORE

Source: DigWatch

Date: 18 February 2024

Japan joins global AI regulation race with comprehensive 2024 legislative push

"The Liberal Democratic Party of Japan is set to present new legislation to regulate generative AI technologies in 2024, according to Nikkei Business Daily. This move by the ruling party is in response to growing concerns about disinformation and rights infringements associated with AI. The party's AI project team plans to draft preliminary rules, which may include penal regulations, for foundation model developers like Microsoft-backed OpenAI GPTs. This initiative follows the European Union's recent progress towards adopting the AI Act, and it coincides with other governments, including the USA and China, exploring ways to regulate the technology." READ MORE

Source: AGBrief

Date: 26 February 2024

Southeast Asia illegal online gaming and scam industries booming since mid-2010s: Monitoring group

"Southeast Asia online gaming and scam industries have been growing since at least 2010, but expansion in the Philippines, Cambodia, Myanmar and Laos was rapid from the mid-2010s, Cyber Scam Monitor (CSM), an independent monitoring group, told AGB. In an interview with AGB, CSM underlined that 'it is not an NGO and has no organizational affiliation', being composed mainly of people from the human rights, anti-trafficking, academic, and media fields." READ MORE

Source: Fiji News

Date: 21 February 2024

Fiji: INTERPOL trains officers in cybercrime response

"Officials from INTERPOL Global Action on Cybercrime Extended (GLACY+) are in the country, conducting an e-Evidence First Responders Training in the Western Division. The training aims to help officers triage digital crimes, handle electronic evidence and maintain its integrity. Acting Divisional Police Commander West – Acting Senior Superintendent of Police, Aisake Kafoa emphasised the importance of staying ahead of cybercrimes, thanking INTERPOL for their support." READ MORE

Source: BNN Breaking

Date: 29 February 2024

Philippine Government Boosts Fight Against Financial Cybercrimes with New Tools

"The Philippine government is stepping up its battle against financial technology (fintech) crimes by acquiring specialized tools, as disclosed by the Cybercrime Investigation and Coordinating Center (CICC). This move is set to significantly enhance the country's ability to trace and combat cybercrimes within the rapidly growing fintech sector. […] Further strengthening the fight against cybercrimes, the Philippine National Police - Anti-Cybercrime Group (PNP-ACG) reported the establishment of additional regional and provincial offices and cybercrime desks across police stations." READ MORE

Source: STORMSHIELD

Date: 28 February 2024

Use of cyber-tools in the Russian-Ukrainian war: a strategic analysis of a major first

"The Russian invasion of Ukraine marked a first in the history of conflict, with the widespread use of cyberattacks. This development has transformed the landscape of the traditional war, raising many questions. We take a closer look at a hybrid cyber-warfare in which the forces involved are a combination of traditional battlefields and a new digital dimension. […] This war in Ukraine has provided an opportunity for hacktivist groups to step up their efforts across the board, from those working on behalf of the Russian state to those defending Ukrainian defence efforts. With cyberspace serving as a new battleground, several hacktivist groups have explicitly aligned themselves with the subject of their political affiliations." READ MORE

Source: The Record

Date: 28 February 2024

Ukraine expects billion-dollar Russian disinformation campaign to peak this spring

"Ukraine's military intelligence unit warned that Russia has poured more than $1 billion into an ongoing disinformation campaign aimed to diminish Western support for Kyiv and sow panic and distrust among Ukrainian citizens. […] Ukraine said it estimated that Russia has spent $250 million to spread anti-Ukrainian narratives on the messaging app Telegram, with the whole campaign costing about $1.5 billion. While Ukraine has labeled Maidan-3 as the most expensive campaign by Russian intelligence, there's no independent research to confirm this." READ MORE

Source: UNDP

Date: 21 February 2024

UNDP and the U.S. Government will equip more police inspectorates in Moldova with modern tools, including for investigating cybercrime

"Police inspectorates in several districts of Moldova will be equipped with modern investigative tools and devices to enhance their capacity to react and respond to public order and security threats. Similarly, National Police subdivisions will benefit from specialized hardware and software solutions to support cybercrime investigations. Mobile police stations will be purchased and adapted for field investigation work, crime prevention and road traffic monitoring." READ MORE

Source: Voice of Europe

Date: 26 February 2024

Albanian advocacy group urges government action against cyber violence targeting women

"An Albanian women's organization is calling on the government to criminalize cyber violence against women following two tragic suicides linked to online harassment this year, Euronews writes. The plea comes after a 27-year-old woman took her own life this month following the blackmail and dissemination of explicit photos by a TikTok influencer she was involved with, as reported by local media. The accused individual, TikToker Altin Çoku, has been arrested and charged with "causing suicide" by the Court of Tirana, with the case shedding light on the growing issue of cyber violence against women in Albania." READ MORE

Source: Bloomberg

Date: 27 February 2024

Microsoft's Mistral AI Investment to Be Examined by EU Watchdog

"Microsoft Corp.'s Mistral AI investment is set to be analyzed by the European Union's competition watchdog at the same time that its deep ties to OpenAI Inc come under regulatory scrutiny. Mistral announced a "strategic partnership" with Microsoft on Monday that includes making the startup's latest artificial intelligence models available to customers of Microsoft's Azure cloud. Microsoft said the investment amounted to €15 million ($16.3 million.) […] That relationship is now under scrutiny from regulators in the UK and EU." READ MORE

Source: Cyber Security Intelligence

Date: 23 February 2024

A European Cybercrime Breakthrough Is Only Half the Battle

"Cybercrime is a global challenge on a massive scale. If cybercrime was a country, it would have one of the largest economies in the world. Statista estimates that the cost of cybercrime was $8.15 trillion in 2023. Meanwhile, 37 per cent of large companies in the UK say they have experienced cybercrime in the past year. Why is the cost of cybercrime so high? Because the first rule of cybercrime is that no one goes to prison." READ MORE

Source: Bitdefender

Date: 27 February 2024

Germany: Cybercriminals Halt Car Body Production at ThyssenKrupp Automotive Division

"Steel production giant ThyssenKrupp has had a run-in with hackers, prompting it to shut down the IT systems at its automotive division. The German conglomerate is one of the world's largest steel producers, with products ranging from machines and industrial services to high-speed trains, elevators, and shipbuilding. ThyssenKrupp's Automotive Body Solutions, which makes car bodies, suffered a cyberattack last week, halting production. […] ThyssenKrupp has yet to issue a complete, official statement on the incident. It is unclear if this was a targeted attack, who the culprits may be, what their intentions were, etc. Over the years, ThyssenKrupp has been the victim of multiple hacking attacks targeting the company's trade secrets." READ MORE

Source: Sentinelone

Date: 22 February 2024

Doppelgänger | Russia-Aligned Influence Operation Targets Germany

"SentinelLabs and ClearSky Cyber Security have been tracking a propaganda and disinformation campaign since late November 2023, highly likely orchestrated by Doppelgänger, a suspected Russia-aligned influence operation network known for its persistent and aggressive tactics. Initially focusing on disseminating anti-Ukraine content following the onset of the Russo-Ukrainian conflict, Doppelgänger has since broadened its scope, targeting audiences in the US, Israel, Germany, and France." READ MORE

Source : rtbf

Date: 20 February 2024

Des hackers russes s'attaquent à plusieurs sites gouvernementaux belges

"Des pirates informatiques russes ont mis hors service un certain nombre de sites web gouvernementaux pendant un certain temps mardi. Le site du Premier ministre Alexander De Croo et celui de la Chambre des représentants ont, entre autres, été brièvement indisponibles mardi après-midi. Via Telegram, le collectif de hackers "NoName057 (16)" a fait savoir qu'il était "parti en visite en Belgique" et qu'il avait mis hors service les sites web du Premier ministre Alexander De Croo, le site internet de Bruxelles et celui de la Chambre. "Nous avons lu que la Belgique, comme un certain nombre d'autres pays russophobes, a fourni une assistance financière au régime criminel de Zelensky au cours de l'année écoulée", explique le collectif de pirates informatiques pro-russes pour justifier cette cyberattaque." READ MORE

Source : CIDJ - Centre d'Information et de Documentation Jeunesse

Date: 20 February 2024

Réseaux sociaux : une loi inscrit le droit à l'image et à la vie privée des enfants dans le Code civil

"Sur internet, les enfants aussi ont droit au respect de leur vie privée. Une loi, adoptée définitivement le 6 février 2024, vise à garantir le respect du droit à l'image des mineurs français à l'heure où de nombreux parents publient des images sur les réseaux sociaux. Il s'agit de sensibiliser ces derniers aux conséquences de ces publications et de les sanctionner en cas de manquement." READ MORE

Source: The Quantum Insider

Date: 26 February 2024

France Advances Quantum Technology Export Controls Under New EU Regulation Framework

"France enacted a comprehensive national control list, directly responding to the emerging disruptive potential — both constructive and destructive — of quantum computing, along with associated disruptive technologies in both civilian and military realms, according to recent information from the French government and computer translated into English. This step, taking effect the month following its publication in the Official Journal of the French Republic on Feb. 8, is in strict adherence to the European Union's Regulation 2021/821 from May 20, 2021, which mandates a unified EU control regime over the export, brokering, technical assistance, transit, and transfer of dual-use items." READ MORE

Source: The Guardian

Date: 27 February 2024

US judge halts government effort to monitor crypto mining energy use

"The US government has suspended its effort to survey cryptocurrency mining operations over their ballooning energy use following a lawsuit from an industry that has been accused by environmental groups of fueling the climate crisis. A federal judge in Texas has granted a temporary order blocking the new requirements that would ascertain the energy use of the crypto miners, stating that the industry had shown it would suffer "irreparable injury" if it was made to comply. The US Department of Energy had launched an "emergency" initiative last month aimed at surveying the energy use of mining operations, which typically use vast amounts of computing power to solve various mathematical puzzles to add new tokens to an online network known as a blockchain, allowing the mining of currency such as bitcoin." READ MORE

Source: CBC News

Date: 26 February 2024

Canada: Long-awaited online harms bill proposes higher sentences for spreading hate online

"The Liberal government is proposing heavier sentences, new regulatory bodies and changes to a number of laws in new legislation to tackle online abuse. The Online Harms Act, tabled Monday, proposes to police seven categories of harmful content online. Those categories include content used to bully a child and content that encourages a child to harm themselves. They also include hate speech, content that incites violence or terrorism, content that sexualizes children or victims of sexual violence, and sexual content that is posted without consent." READ MORE

Source: Reuters

Date: 24 February 2024

Canadian federal police says they were targeted by cyberattack

"Canadian federal police said on Friday their systems were targeted by an "alarming" cyberattack but there was no impact on operations and no known threat to the safety of Canadians […]The Royal Canadian Mounted Police said they launched a probe into the attack and were trying to determine the extent of the breach, adding there were no known impacts on intelligence services. The Canadian government said late last month that its foreign affairs department had suffered a data breach, opens new tab and that there had been unauthorized access to personal information of users including employees." READ MORE

Latest reports

- ECHR, CASE OF PODCHASOV v. RUSSIA (Application no. 33696/19), 13 February 2024
- Cellebrite, Collaboration Between Digital, Investigation Units is Key to Case Success, 16 February 2024
- Microsoft, Technology industry to combat deceptive use of AI in 2024 elections, 16 February 2024
- Finances online, 73 Important Cybercrime Statistics: 2024 Data Analysis & Projections, 16 February 2024
- Truelist, Cybercrime Statistics – 2024, 17 February 2024
- ECHR, AFFAIRE DANILEȚ c. ROUMANIE (Requête no 16915/21), 20 February 2024
- Kaspersky, Ransomware: the most high-profile attacks of 2023, 20 February 2024
- Sophos, LockBit: Lessons learned on winning the war on cybercrime, 21 February 2024
- EIOPA, AI Act and its impacts on the European financial sector, 21 February 2024
- The Hindu, India is the 80th most targeted country worldwide in cybercrime: Report, 21 February 2024
- SonicWall, Latest Threat Intelligence Navigates the Relentless Surge in Cybercrime, 21 February 2024
- EFF, Unregulated, Exploitative, and on the Rise: Vera Institute's Report on Electronic Monitoring, 21 February 2024
- Dataconomy, Coûts mondiaux des cyberattaques en 2024 et dans le futur, 22 February 2024
- WEF, 3 trends set to drive cyberattacks and ransomware in 2024, 22 February 2024
- Statista, Cybercrime Expected To Skyrocket in Coming Years, 22 February 2024
- CyberPreventys, Etude : les TPE et PME surestiment leur niveau de protection face aux cyberattaques, 22 February 2024
- CISA, Resources-for-Cybersecurity-Clinics-508c.pdf, 23 February 2024
- CISA, Cyber Threats to Medical Technology and Communication Technology Protocols, 23 February 2024
- Sophos, ConnectWise ScreenConnect attacks deliver malware, 23 February 2024
- EPIC (Electronic Privacy information Center), Summary: What does the European Union Artificial Intelligence Act Actually Say?, 23 February 2024
- KrebsonSecurity, FBI's LockBit Takedown Postponed a Ticking Time Bomb in Fulton County, 25 February 2024
- CISA, SVR Cyber Actors Adapt Tactics for Initial Cloud Access, 26 February 2024
- Bleepingcomputer, Hackers exploit 14-year-old CMS editor on govt, edu sites for SEO poisoning, 26 February 2024
- Cyberseguridad PYME, Los mayores ciberataques de 2023 principales filtraciones de datos y ataques de ransomware, 27 February 2024
- US Department of Justice, Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations, 27 February 2024
- Talos, TimbreStealer campaign targets Mexican users with financial lures, 27 February 2024

- Security Affairs, Russia-linked apt28 compromised Ubiquiti EdgeRouters to facilitate cyber operations, 28 February 2024
- CISA, Fact Sheet: Top Cyber Actions for Securing Water Systems, 28 February 2024
- KrebsonSecurity, Calendar Meeting Links Used to Spread Mac Malware, 28 February 2024
- ENISA, Best Practices for Cyber Crisis Management, 28 February 2024
- Global Initiative, Criminal exploitation of deepfakes in South East Asia, 29 February 2024
- Hipther, IDTechEx Reports on Quantum Technology: The Double-edged Sword in the Fight Against Cybercrime, 29 February 2024
- Schneier, How the "Frontier" Became the Slogan of Uncontrolled AI, 29 February 2024
- Channel News Asia, AI in Southeast Asia: As bad actors gain new high-tech weapons, so too for the defenders, 29 February 2024
- Cointelegraph, Spot Bitcoin ETF volumes shatter record with massive $7.7B traded, 29 February 2024
- Tech Coalition Safe Online Research Fund, Tech Platforms Used by Online Child Sexual Abuse Offenders, February 2024
- CrowdStrike, 2024 Global Threat Report, February 2024
- Arkose Lab, Bot Abuse Analysis and other Fraud Benchmarks - Financial Services Industry, February 2024

Upcoming events

- 4 March 2024, C-PROC/TUNISIA, (in person), Contribution to the Launching Conference of the 'Rule of Law Youth Network' (RoLYN) with a presentation and discussion on the tools offered by the Budapest Convention and its protocols, CyberSouth+
- 5 March 2024, C-PROC/TUNISIA, (in person), Meeting with the Ministry of Foreign Affairs to discuss the ongoing revision of the decree-law 54/2022 and a possible bi-lateral capacity building project on cybercrime, CyberSouth+
- 5 March 2024, C-PROC/TUNISIA, (in person), Meeting with the Italian Embassy to present the Council of Europe activities in Tunisia in the field of justice and cybercrime, CyberSouth+
- 6 March 2024, C-PROC/TUNISIA, (in person), Meeting with DCAF representatives in Tunisia to co-ordinate and discuss possible co-operation under CyberSouth+ project, CyberSouth+
- 11-13 March 2024, C-PROC/ECUADOR, (in-person), Advisory workshop on cybercrime strategies, GLACY-e
- 14 March 2024, C-PROC/LIBYA, (online), Meeting with the Ministry of Foreign Affairs representatives to present and discuss the CyberSouth+ project, CyberSouth+
- March 2024, C-PROC, (online), further developments of the Octopus platform, Octopus
- March 2024, C-PROC, (*online*), further developments of the CYBOX platform, Octopus
- March 2024, C-PROC, *(online)*, maintaining cyberviolence resource, 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