Cybercrime Digest

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

16–30 November 2022

Source: Council of Europe

Date: 30 November 2022

Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence

"On 30 November 2022, during the 27th Plenary of the Cybercrime Convention Committee (T-CY) in Strasbourg, France, a further six States signed the Second Protocol to the Budapest Convention. Croatia, Moldova, Slovenia, Sri Lanka, Ukraine and the United Kingdom joined 24 other countries that had signed it earlier this year. The Protocol on enhanced cooperation and disclosure of electronic evidence (CETS 224) will enter into force once five States will have ratified it. Brazil, at the same event, deposited the instrument of accession to the Convention on Cybercrime. With Brazil becoming a Party, 68 States are now able to cooperate with each other within the framework of this Convention." READ MORE

RELATED ARTICLES:

Council of Europe, Enhanced co-operation and disclosure of electronic evidence: new countries join additional Protocol to Cybercrime Convention, 30 November 20222

Agencia Brasil, Brazil joins Budapest convention against cybercrime, 1 December 2022

MercoPress, Brazil joins Budapest Convention to fight cybercrime, 1 December 2022

Source: Council of Europe

Date: 29 November 2022

Ransomware: New Guidance Note by the T-CY

"The Cybercrime Convention Committee just adopted a guidance note on "ransomware". This new GN shows how the provisions of the Convention on Cybercrime, and its new Second Additional Protocol can be used to criminalize, investigate and prosecute ransomware-related offences and to engage in international cooperation. "In our meeting today, numerous Parties and observers to the Budapest Convention have stated that they have been targets of major ransomware attacks in recent months. This Guidance Note once more demonstrates that the Convention on Cybercrime is sufficiently versatile to also address offences related to ransomware," , said Alexander Seger, Executive Secretary of the Committee. READ MORE

Source: European Commission

Date: 29 November 2022

Commission welcomes political agreement to strengthen cross-border access for criminal investigations

"The European Commission welcomes the provisional political agreement reached today by the European Parliament and the Council on the new rules for sharing of e-evidence across the EU. This agreement will lead to the formal adoption of a Directive and a Regulation to govern these provisions, following the Commission's proposal. Currently, the Member States' authorities must rely on lengthy judicial cooperation procedures to obtain electronic evidence, with the related risks of the sought data being moved or deleted, or on procedures of voluntary cooperation with service providers involving a lack of reliability, transparency, accountability and legal certainty." READ MORE

RELATED ARTICLE:

Euractiv, EU settles rules for accessing electronic evidence across borders, 29 November 2022

Source: Europol

Date: 28 November 2022

International operation shuts down websites offering counterfeit goods and pirated content

"Law enforcement agencies from 27 countries* participated in the 13th edition of Operation In Our Sites, a Europol-coordinated operation to take down websites offering counterfeit goods or involved in online piracy. The recurring operation, which is supported by Eurojust and INTERPOL, targets, investigates and seizes websites hosting a variety of illicit content. The main issues continue to be intellectual property infringement on trademarks, as well as on copyrighted content available on internet protocol television (IPTV) and movie streaming services, peer-to-peer sharing platforms and hosting websites. Key findings of the operation that took place from 1 May to 14 November also show that more counterfeit products are being assembled within the European Union's borders and that intellectual property crime is closely intertwined with serious and organised crime." READ MORE

Source: Council of Europe

Date: 24 November 2022

The Netherlands makes a voluntary contribution to the Octopus Project

"The Netherlands, through the Ministry of Justice and Security, made a voluntary financial contribution of EUR 50 000 to the Octopus Project implemented by the Council of Europe until 31 December 2024. The project, based on voluntary contributions from State Parties and Observers to the Convention on Cybercrime, aims to support countries worldwide in strengthening their criminal justice capacities in line with the Convention on Cybercrime, its protocols and related standards, as well as to address additional challenges that came to the forefront in the course of 2020. In particular, following opening for signature of the Second Additional Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence in May 2022, the project seeks to support States in its ratification and implementation." READ MORE

Source: Council of Europe

Date: 30 November 2022

Electronic evidence of war crimes and the role of journalists, media and social media

“The webinar "Electronic evidence of war crimes. The role of journalists, media and social media” has been held on 25 November 2022 in Strasbourg organized by the Group of Friends on the Safety of Journalists and Media Freedom in Strasbourg and the Council of Europe. The Ukrainian law enforcement bodies reported that during nine months of war, there are 67005 crimes registered related to the aggression of the Russian Federation, among which 46563 are war crimes. Besides the work of the law enforcement bodies, there are more actors who track atrocities in Ukraine, and these are the journalists and the media. Their role, as well as the role of social media, human rights activists and ordinary citizens is huge in collecting, preserving and verifying open-source information related to the war crimes.” READ MORE

Source: Politico.eu

Date: 23 November 2022

European Parliament website hit by cyberattack after Russian terrorism vote

“The European Parliament website on Wednesday faced a "sophisticated" cyberattack disrupting its services moments after members voted to declare Russia a state sponsor of terrorism. "I confirm that the Parliament has been subject to an external cyber-attack, but the Parliamentary services are doing well to defend the Parliament," Dita Charanzová, Czech MEP and Parliament vice president responsible for cybersecurity, said in a statement. Another senior Parliament official, requesting not to be named, said “it might be the most sophisticated attack that the Parliament has known so far.” READ MORE

RELATED ARTICLE:

Euronews, EU Parliament website hacked after MEPs passed critical Russian resolution, 23 November 2022

Source: L’Usine Digitale

Date: 25 November 2022

Interpol saisit 130 millions de dollars provenant de la cybercriminalité

“Une opération menée par Interpol, à laquelle ont concouru 30 pays dont la France, a permis d'arrêter près d'un millier de suspects impliqués dans des crimes financiers commis en ligne, avec le soutien de la Corée du Nord. 130 millions de dollars. C'est la somme qu'a permis d'intercepter une opération de police menée par Interpol, en coordination avec 30 pays dont la France. Cette opération, "Haechi III", a abouti à l'arrestation de 975 individus et à la résolution de 1600 affaires de phishing vocal, d'arnaques, d'extorsion, de fraudes et de blanchiment issu de jeux d'argent illicite, commis en ligne et soutenus par la Corée du Nord, a annoncé l'organisation internationale de police criminelle le 24 novembre. Coordonnée par le bureau du crime financier et de l'anti-corruption d'Interpol, l’opération Haechi III a duré plus de cinq mois, du 28 juin au 23 novembre.” READ MORE

Source: euractiv.com

Date: 21 November 2022

EU Council discusses cross-border removal orders to fight child pornography

"A new compromise text by the Czech EU Council presidency has expanded the original proposal for tackling online child sexual abuse material to include a mechanism for dealing with cross-border content removal. In a newly added section, the regulation now includes provisions to cover cases where the relevant service providers are established in different member states to the one in which the victim filing the order is established.[…] The Commission's proposal was released in May to place obligations on online service providers to detect, report and remove child sexual abuse material (CSAM) on their platforms, but it has spurred controversy over its privacy implications." READ MORE

Source: Europol

Date: 24 November 2022

Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests

"Judicial and law enforcement authorities in Europe, Australia, the United States, Ukraine, and Canada have taken down a website that allowed fraudsters to impersonate trusted corporations or contacts to access sensitive information from victims, a type of cybercrime known as 'spoofing'. The website is believed to have caused an estimated worldwide loss in excess of GBP 100 million (EUR 115 million). In a coordinated action led by the United Kingdom and supported by Europol and Eurojust, 142 suspects have been arrested, including the main administrator of the website." READ MORE

RELATED ARTICLE:

Eurojust, Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests, 24 November 2022

Source: euractiv.com

Date: 22 November 2022

EU Council mulls broad national security carveouts in IoT cybersecurity law

"The Czech presidency of the EU Council has circulated the first compromise on the Cyber Resilience Act, dated 18 November and obtained by EURACTIV, making hefty editing to the proposal's scope and free movement clause. The Cyber Resilience Act is horizontal legislation intended to introduce essential cybersecurity requirements for connected devices and their related services. Since the proposal was published in September, national representatives in the EU Council have been engaged in preliminary discussions. The new text will be discussed at the Horizontal Working Party on Cyber Issues, a preparatory body in the EU Council, on Wednesday (23 November)." READ MORE

Source: Acento.com.do

Date: 21 November 2022

Joel Santos resalta prioridades de República Dominicana en materia de ciberseguridad

"El ministro de la Presidencia, Joel Santos Echavarría, resaltó las prioridades de República Dominicana en materia de ciberseguridad, durante su participación en la Cumbre Latam CISO 2022, encuentro que reunió a los líderes de ciberseguridad más relevantes de América Latina y el Caribe para discutir las amenazas y las tendencias más críticas y desafiantes en el mundo digital. En ese sentido, el ministro explicó que como país es importante mantener la resiliencia y crear conciencia colectiva sobre el tema de la seguridad cibernética, generar instrumentos legales y normativos que permitan la ejecución de las líneas de acción, mantener colaboración con los demás Estados y cumplir con los estándares internacionales que permitan un ecosistema de ciberseguridad adecuado." READ MORE

Source: qcostarica.com

Date: 15 November 2022

Costa Rica: Seniors targeted by cybercriminals

"Cybercrime does not forgive social rank or age and therefore, older adults have become easy prey for antisocials, who use increasingly convincing social engineering techniques to access sensitive information. And it is that the theft of financial information can occur due to ignorance or overconfidence, which leads to the execution of modalities such as "phishing" or "twinning" of websites." READ MORE

Source: Noticias enfasis

Date: 17 November 2022

México es el primer país de América Latina en número de ciberataques

"El senador Ricardo Monreal, consideró urgente para el país contar con una Agencia Nacional en Ciberseguridad, un tema no solo de seguridad nacional, sino un factor para el desarrollo social y económico del país. En la sesión inaugural del Foro virtual "Hacia un Ciberespacio más Seguro", el presidente de la Junta de Coordinación Política señaló que México necesita comprometerse con sus socios nacionales, regionales e internacionales para combinar recursos, iniciativas de múltiples partes interesadas y facilitar el intercambio de información, para garantizar la seguridad en el ciberespacio y aprender de las mejores prácticas." READ MORE

Source: bankinfosecurity.com

Date: 17 November 2022

Australia Unveils Plan to Counter Global Cybercrime Problem

“Following a spate of cyberattacks and data breaches affecting millions of Australians, the government’s cybersecurity minister this week announced the formation of a task force that will hunt down hackers and said she is contemplating a ban on ransomware payments Australia Cyber Security Minister Clare O'Neil announced the formation of the Joint Standing Operation task force, which brings together experts from the Australian Federal Police and the Australian Signals Directorate. The task force merges domestic police and foreign intelligence resources to provide assistance to victims and also to take down international cybercriminals. The Joint Standing Operation will "investigate, target and disrupt cybercriminal syndicates with a priority on ransomware threat groups," according to a joint news release.” READ MORE

Source: tribune.com.pk

Date: 21 November 2022

Should Pakistan sign the Budapest Convention?

“With a high-powered committee probing the cyber security breach at the Prime Minister’s office and being entrusted with preparing a legal framework for the seamless security of government assets, it has sparked a debate about whether Pakistan should finally join the famous Cybercrime Convention or not. The Cybercrime Convention, or the Budapest Convention, took a global approach to cybercrime that involved harmonising national law related to cyber security and electronic crimes, improving forensic abilities, and enabling international cooperation between law enforcement agencies.” READ MORE

Source: The Guardian

Date: 29 November 2022

Vanuatu officials turn to phone books and typewriters, one month after cyber attack

“One month after a cyber-attack brought down government servers and websites in Vanuatu, frustrated officials were still using private Gmail accounts, personal laptops, pen and paper, and typewriters to run the government of the prime minister, Ishmael Kalsakau, who came into office just a few days after the crash. The malware attack on state networks has caused delays in communication and coordination in the Pacific island nation of 314,000 people and 80 islands. People resorted to the online Yellow Pages or the hard copy phone directory to locate government phone numbers. Some offices were running from their Facebook pages and Twitter. The problems began about a month ago, when suspicious phishing activity was first noticed in emails to the Ministry of Finance, according to a financial analyst who works closely with the ministry’s cybersecurity teams.” READ MORE

Source: orfonline.org

Date: 30 November 2022

The AIIMS cyberattack reflects India’s critical vulnerabilities

“The frequency and targets of cyberattacks on India are becoming increasingly serious. Earlier in the month of November, Central Depository Services (India) Limited (CDSL) detected a malware in some of its internal machines though the CSDL claimed that “there is no reason to believe that confidential information or investor data has been compromised.” In the latest such attack, just a week ago, one of India’s top medical institutions—the All India Institute of Medical Sciences (AIIMS) Delhi—came under cyberattack. Though India has been paying greater attention to cyber security, the rising number of attacks on India should be very worrying to Indian security managers.” READ MORE

Source: Interpol

Date: 25 November 2022

Operation across Africa identifies cyber-criminals and at-risk online infrastructure

“Law enforcement officials from 27 INTERPOL countries joined forces in the Africa Cyber Surge Operation to counter cybercrime across the continent. Against the backdrop of the huge financial losses suffered by companies, businesses and individuals, the four-month operation (July to November 2022) saw officers detect, investigate and disrupt cybercrime through coordinated law enforcement activities utilizing INTERPOL platforms, tools and channels, in close cooperation with AFRIPOL. Coordinated from an INTERPOL Command Centre in Kigali, Rwanda, the operation focused on removing the enablers of cybercrime.” READ MORE

Source: The Guardian

Date: 27 November 2022

Gangs of cybercriminals are expanding across Africa, investigators say

“Police and investigators fear organised gangs of fraudsters are expanding across sub-Saharan Africa, exploiting new opportunities as a result of the Covid-19 pandemic and the global economic crisis to make huge sums with little risk of being caught. The growth will have a direct impact on the rest of the world, where many victims of “hugely lucrative” fraud live, senior police officials have said. Experts attribute the surge in cybercrime in Africa to rapid growth of internet use at a time when police forces and criminal justice systems have been weakened by the economic consequences of a series of major challenges. “The Covid-19 pandemic has accelerated digitalisation around the world, but as life has shifted increasingly online, cybercriminals have exploited the opportunity to attack vital digital infrastructure,” said Prof Landry Signé, a senior fellow at the Brookings Institution and author of a recent report on the problem. “States across Africa have emerged as a favourite target of cybercriminals, with costly consequences.”” READ MORE

Source: wearetech.africa

Date: 25 November 2022

La Côte d'Ivoire durcit sa loi sur la cybercriminalité

"La cybercriminalité gagne du terrain en Afrique. Escroqueries en ligne, menaces d'attaques d'ampleur, l'Afrique subsaharienne est présentée comme particulièrement vulnérable face à la cybercriminalité. Le gouvernement ivoirien veut mettre fin à toutes les formes de menaces qui minent son cyberespace. Le projet de loi modifiant les articles 17, 33, 58, 60,62 et 66 de la loi N° 2013-451 du 19 janvier 2013, relative à la lutte contre la cybercriminalité a été défendu le mercredi 23 novembre par Amadou Coulibaly, le ministre de la Communication et de l'Economie numérique. A l'unanimité, la loi a été votée par des députés membres de la Commission des affaires générales et institutionnelles." READ MORE

Source: lopinion.ma

Date: 15 November 2022

Cybersécurité : Le Maroc et Israël avancent dans leur partenariat

"Le numérique au Maroc a connu des défis sécuritaires surtout depuis l'année 2021, année où les autorités marocaines ont recensé 577 menaces de Cybersécurité. La digitalisation est vigoureusement portée par un Internet plus accessible, mais représente de nos jours une faiblesse potentielle en matière de sécurité. La Cybersécurité fait donc partie intégrante des secteurs qui s'inscrivent dans les partenariats stratégiques entre Rabat et Israël. Elle consiste principalement à protéger les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. Il est à noter que le Royaume fait partie des pays les plus sûrs de la région MENA puisqu'il se classe 5ème en matière de Cybersécurité dans le Top africain." READ MORE

Source: businessday.ng

Date: 18 November 2022

Nigeria recorded a 174% increase in cybercrimes in six months, here's why you should be bothered

"In Africa, the peril of cybercrimes recorded a massive rise in the first six months of 2022, "with phishing and scams hitting 438 per cent and 174 per cent in Kenya and Nigeria, respectively", the Guardian Newspapers. reported on August 3, 2022. To truly understand the magnitude and far-reaching effects of this global menace, various experts have estimated the cost impact to reach 7 trillion US Dollars by the end of this year. Worse still, numerous studies have estimated a yearly 15 per cent per year increase in global cybercrime losses over the next five years, reaching 10.5 trillion US Dollars annually by 2025." READ MORE

Source: joint-research-centre.ec.europa.eu

Date: 24 November 2022

New website to monitor the uptake of key internet standards across the EU

"The Commission launches a new website to monitor the deployment of five categories of key internet communication standards in the EU, considered essential to achieve the EU vision of a free, open, accessible and secure global internet. The EU's Internet Standards Deployment Monitoring website features the set of internet standards that are considered to be key to supporting a free, open and global internet, and which contribute to securing internet communications and support the evolution and resilience of the Internet." READ MORE

Source: lesechos.fr

Date: 18 November 2022

Cybercriminalité: l'Ile-de-France déploie son bouclier défensif

"[…]Pour établir son « Observatoire de la performance cybersécurité » des communes franciliennes, la région a fait appel à la start-up Board of Cyber, experte en gestion du risque numérique. Cette dernière vient de réaliser un gigantesque « scan » de la performance en termes de cybersécurité des 716 communes d'Île-de-France comptant plus de 1.000 habitants et des 71 intercommunalités. Selon une première tendance, plus de la moitié des communes et intercommunalités doivent faire des efforts très importants pour améliorer leur sécurité numérique." READ MORE

Source: news.sky.com

Date: 18 November 2022

UK: Children coerced into most severe form of sexual abuse online, report finds

"Children as young as seven are being coerced by abusers into filming themselves carrying out the most severe forms of child sexual abuse material, a charity has warned. Analysts at child protection charity the Internet Watch Foundation (IWF) found nearly 900 instances of Category A child sexual abuse material in just five days. It is urging the government to return the repeatedly delayed Online Safety Bill to parliament. The IWF's chief executive Susie Hargreaves said the charity shared details of the material to "drive home the stark reality of the situation" and said the government must reintroduce the Online Safety Bill to protect children." READ MORE

Latest reports

- Republic.com, Cyber Ready: Africa’s Response to Growing Cyber Threats, October-November 2022
- Arstechnica.com, How North Korea became a mastermind of crypto cybercrime, 15 November 2022
- EUROPOL, EU IRU Transparency Report 2021, 17 November 2022
- OAS.org, Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA, 17 November 2022
- EUROPOL, Child sexual abuse: new guidelines for first responders, 18 November 2022
- Dig.watch, Ukraine conflict: Digital and cyber aspects, 20 November 2022
- Sophos, SOPHOS 2023 Threat Report, 21 November 2022
- Reuters, Crypto exchanges enabled online child sex-abuse profiteer, 23 November 2022
- Enisa Europa, NIS Investments 2022, 23 November 2022
- BBC, The Kenyans lured to become unwitting 'love' fraudsters, 26 November 2022
- H50.es, Falsedades online: el delito de guante blanco que golpe a los aficionados al entretenimiento, 28 November 2022
- Council of Europe, Ransomware: New Guidance Note by the T-CY, 29 November 2022
- INTERPOL, Rapport de synthèse d’INTERPOL sur les tendances mondiales de la criminalité en 2022, 30 November 2022
- Bankless times, 54% Of All Reported Cybercrime Cases Result From Fraud, Online Shopping, and Online Banking, 30 November 2022

Upcoming events

- 5 December, C-PROC/GERMANY, (*in-person*), Cyber Diplomacy Training: A Framing Discussion: Cybercrime in Cyberspace, GLACY+
- 5-9 December, C-PROC/TURKIYE, (*in-person*), International Cybercrime Conference, 7th edition, iPROCEEDS-2
- 6 December, COUNCIL OF EUROPE/STRASBOURG, (*in-person and online*), Joining forces: applying the cybercrime frame to digital violence against women, Violence Against Women Division in cooperation with the Cybercrime Division
- 6-9 December, C-PROC/GHANA, *(in-person),* Support the national delivery of the Introductory Judicial Training on Cybercrime and Electronic Evidence, co-organised with OCWAR-C, GLACY+
- 6-7 December, C-PROC/ IRELAND, *(in-person),* UCD Conferring Ceremony and supporting workshops for the Master Programme students, CyberEast, iPROCEEDS-2
- 7 December, C-PROC/BELGIUM, (*in-person*), CyberSouth 9th Steering Committee Meeting, CyberSouth
- 7 December, C-PROC/TURKIYE*, (in-person*), Domestic public/private meeting on cooperation between criminal justice and ISPs, iPROCEEDS-2
- 9 December, C-PROC/PHILIPPINES*, (hybrid),* National Cybercrime Convention, GLACY+
- 10-31 December, C-PROC/LEBANON, (*on-line*), Finalisation and validation of the basic judicial training course on cybercrime and e-evidence for its adoption onto the national curricula, CyberSouth
- 11-14 December, C-PROC/ALGERIA, (*in-person*), Finalisation and validation of the basic and advanced judicial training courses on cybercrime and e-evidence for their adoption into the national curricula, CyberSouth
- 12 December, C-PROC/Eastern Partnership, *(hybrid),* CyberEast project Steering Committee meeting, CyberEast
- 13 December, C-PROC/ROMANIA, *(in-person),* Southeast Europe Police Chiefs Association Conference, iPROCEEDS-2
- 13-14 December, C-PROC/Eastern Partnership, *(hybrid),* Regional Meeting on Cyber Reporting and Data Sharing, CyberEast
- 13-15 December, C-PROC/SERBIA, (*in-person*), Basic training course on cybercrime, electronic evidence, and online crime proceeds, iPROCEEDS-2
- 15 December, C-PROC/NORTH MACEDONIA, (in-person), Domestic public/private meeting between service providers and criminal justice authorities, iPROCEEDS-2
- 15 December, C-PROC/SERBIA, (*in-person*), Domestic workshop on dealing with electronic evidence in international investigations, iPROCEEDS-2
- 15 December, C-PROC, (*on-line*), Webinar on the First Additional Protocol to the Budapest Convention, Octopus project

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime