Cybercrime Digest

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

01 – 17 December 2021

Season's greetings and best wishes for a happy and healthy holiday period from the Cybercrime Programme Office of the Council of Europe.

We are happy to have been able to work on cybercrime with you in 2021 despite the on-going COVID-19 pandemic, and look forward to continuing our cooperation in 2022.

Source: Council of Europe

Date: 16 Dec 2021

Congress of Brazil approves accession to the Budapest Convention

"On 15 December, the Senate of Brazil approved accession to the Budapest Convention. This crucial step will permit the Government of Brazil to deposit the instrument of accession and become a Party to this treaty any time soon, and thus to cooperate effectively on cybercrime and electronic evidence with currently 66 other Parties. Brazil is now also a priority country for capacity building and tailor-made technical assistance activities for criminal justice authorities will be further enhanced." READ MORE

RELATED ARTICLES:

Senado Noticias, Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético, 15 December 2021

Directorio legislativo, Foreign Affairs Committee approves draft adhesion to the Budapest convention on Cybercrime, 9 December 2021

Source: Council of Europe

Date: 8 Dec 2021

Fiji and Vanuatu invited to join the Budapest Convention on Cybercrime

"Fiji and Vanuatu were invited today to accede to the Budapest Convention on Cybercrime. Thus, 80 States are now either Parties (66), or have signed it or been invited to accede (14). The authorities of Fiji and of Vanuatu have been cooperating with the Council of Europe in cybercrime matters for several years. With regard to Fiji this included cooperation on the reform of domestic legislation leading to the enactment of the "Cybercrime Act 2021" in February 2021. […] Cooperation on the reform of domestic legislation in Vanuatu led to the adoption of "Cybercrime Act No. 22 of 2021" in June 2021 that entered into force in September 2021. Domestic legislation of Fiji and of Vanuatu is now broadly in line with the Budapest Convention on Cybercrime." READ MORE

Source: US Department of Homeland Security

Date: 16 Dec 2021

Joint U.S.-EU statement following the U.S.-EU Justice and Home Affairs Ministerial Meeting

"On 16 December 2021, the U.S.-EU Ministerial Meeting on Justice and Home Affairs took place in Washington D.C. [...] The United States and the European Union stated their determination to preserve the Budapest Convention on Cybercrime as the primary instrument for international cooperation on cybercrime and expressed support for its recently adopted Second Additional Protocol to enhance cooperation on cybercrime and e-evidence. They further committed to consult each other and cooperate closely in the negotiations on a future United Nations international legal instrument on cybercrime." READ MORE

Source: Council of the European Union

Date: 15 Dec 2021

Joint Declaration of the Eastern Partnership Summit

"The heads of state or government of the Republic of Armenia, the Republic of Azerbaijan, Georgia, the Republic of Moldova and Ukraine, the representatives of the European Union and the heads of state or government of its member states met in Brussels on 15 December 2021. [...] As regards cyber resilience and cybercrime, a strengthened framework for identifying and assessing hybrid threats is the key target, along with strengthening partners' capacities to tackle cybercrime and increase cyber resilience, with the Council of Europe's Budapest Convention as a baseline. This will be accomplished through improving alignment with EU legal, institutional and cybercrime policy frameworks, running training programmes on cybercrime and electronic evidence, doubling cybercrime-relevant operations involving partner countries and introducing Europol's internet organised crime threat assessment methodology, where appropriate." READ MORE

Source: EUobserver

Date: 7 Dec 2021

Using Istanbul Convention to stop online abuse of women

"Monitoring by the Council of Europe's group of experts on action against violence against women and domestic violence (GREVIO) over the past few years indicates increasing online violence and use of technologies against women and girls. We document digitally-perpetrated violence, from forced 'sexting' and online stalking, to doxing (sharing personal information online, without consent and to encourage abuse), impersonation (creating an online presence in someone else's name) and image-based abuse. […] Our recommendation complements the Istanbul Convention with specific guidance on how to apply the treaty in a digital context. […] It furthermore recommends reviews of existing relevant legislation with the possible adoption of new legislation to prevent, provide protection from and prosecute the digital dimension of violence against women, with respect to the standards of the Istanbul Convention and other relevant treaties, including the Budapest Convention, the Council of Europe treaty against cybercrime that was opened for signature 20 years ago." READ MORE

Source: Europol

Date: 10 Dec 2021

Thousands gather virtually to share knowledge of virtual assets-based money laundering and other crypto-enabled crimes

"The 5th Global Conference on Criminal Finances and Cryptocurrencies on 7-8 December 2021, co-organised by the Basel Institute on Governance, INTERPOL and Europol, saw several thousand participants from the public and private sectors gathering to exchange knowledge on virtual assets-based money laundering and related risks in the crypto sphere. Overall, fast and cooperative action by governments, law enforcement, regulators and the private sector is essential to tackle the risks and keep this dynamic industry safe for all. Virtual assets-based money laundering and other crypto-enabled crimes are threats not only to users and financial markets, but also to the dynamism and innovation of the sector itself." READ MORE

REALTED ARTICLE:

Interpol, Cryptocurrency crime: preventing the misuse of virtual assets by organized crime for money laundering, 9 December 2021

Source: La Tribuna

Date: 7 Dec 2021

Google bloquea una red de ciberdelincuencia que «secuestraba» un millón de dispositivos

"Google reveló este martes que ayudó a bloquear la amenaza de una red de ciberdelincuencia con el control de cerca de un millón de dispositivos electrónicos con los cuales se cometían cibercrímenes, al tiempo que señaló a piratas que operan desde Rusia de ser los responsables. […] Google señaló que la red maliciosa incluía aproximadamente un millón de dispositivos que utilizan Windows en todo el mundo para cometer ataques como el robo de información y credenciales, y se dirigía a usuarios en Estados Unidos, India, Brasil y el sureste de Asia." READ MORE

RELATED ARTICLE:

TechXPLOR, Google disrupts cybercrime web infecting 1 mn devices, 8 December 2021

Source: Eurojust

Date: 9 Dec 2021

Borders, Bytes and Brokering Future Agreements: News from the Fourth SIRIUS Conference

"The SIRIUS project, a cross-border intelligence-sharing platform co-implemented by Europol and Eurojust, in close partnership with the European Judicial Network, concluded its fourth annual conference this week. […] The pandemic-associated rise in online criminality has underscored the importance in international judicial cooperation on sharing electronic evidence. Over the course of the three days, participants discussed areas where gathering electronic evidence has become increasingly important since the outset of the COVID-19 pandemic, such as in relation to cryptocurrencies and crypto-exchanges used in money laundering. Other sessions covered increased European cooperation with law enforcement counterparts in Asia and North America, and the developments in European technical capabilities in fighting cybercrime." READ MORE

Source: BusinessTech

Date: 2 Dec 2021

South Africa's new cybercrime laws have been partially introduced

"President Cyril Ramaphosa has signed the Cybercrimes Bill into law, with parts of the bill taking effect from 1 December 2021. […] The Cybercrimes Act defines three types of harmful messages that have been criminalised in South Africa. They are messages which: Incite damage to property or violence; Threaten people with damage to property or violence; Unlawfully contain an intimate image. In addition to criminalising certain harmful messages, the Act also includes definitions for cyber fraud, forgery, extortion, and theft of incorporeal property. […] Commenting on the new legislation, justice minister Ronald Lamola said the Act streamlines the laws which deal with cybercrime into a single law that criminalises conduct considered to be cybercrimes. The Act also criminalises the disclosure of data messages which are harmful and provides for protection orders to protect victims against harm. The Act also regulates the powers to investigate cybercrimes." READ MORE

Source: DW

Date: 6 Dec 2021

Forum de Dakar : la cybercriminalité au centre des débats

''Le Forum International de Dakar sur la Paix et la Sécurité en Afrique s'est penché lundi sur la cybercriminalité. Le cyber espace en Afrique de l'Ouest est bien occupé par les terroristes, constatent les participants à ce forum. Dans le Sahel, des groupes armés parviennent à communiquer sur les réseaux sociaux. [...] La réponse à cette tendance inquiétante est triple. Selon des experts en cybersécurité, elle se manifeste tant au niveau législatif, organisationnel qu'infrastructurel avec des politiques au niveau continental ou sous-régional comme la convention de Malabo. Ces outils permettent aux Etats de renforcer leurs politiques de lutte contre la cybercriminalité, les agences nationales de cybersécurité, les unités de police et des centres de réponse spécialisés dans le domaine de cybersécurité.'' READ MORE

Source: Council of Europe

Date: 2 Dec 2021

CyberSouth: Second Regional Workshop on the Second Additional Protocol to the Budapest Convention

"The second regional workshop, in the series dedicated to the Second Additional Protocol (SAP) to the Budapest Convention, organized by the CyberSouth project, took place on 15 December 2021. The workshop focused on the rationale and applicability of the SAP articles on emergency mutual legal assistance, video conferencing and joint investigation teams and joint investigations, as part of the procedures pertaining to international cooperation in the absence of applicable international agreements. Furthermore, the conditions and safeguards that State Parties shall foresee in their domestic law, in order to ensure adequate protection of human rights and freedoms were also touched upon.'' READ MORE

Source: The Guardian

Date: 10 Dec 2021

Nigeria: Cybercrime may become next pandemic

"Cybersafe Foundation, a cyber-security awareness creator, has called for more awareness in tackling the growing menace of cybercrime in Nigeria. […] While it was earlier revealed at another forum that Nigeria had lost about N5.5 trillion to fraud and cybercrimes in 10 years, the experts at the Cybersafe forum, in their various presentations warned that cyber security threats and attacks are not going away, as the phenomenon could constitute the next pandemic, spelling out dangers to corporate bodies, government and individuals refusing to create barricades and walls for their platforms, digital tools and applications against cyber-attacks." READ MORE

Source: Medias 24

Date: 13 Dec 2021

Maroc : Piratage, sextorsion, pornographie enfantine: les chiffres de la cybercriminalité en 2020

"La présidence du ministère public mise sur la coopération internationale pour contrer la cybercriminalité. L'institution de Hassan Daki appelle les parquetiers à activer davantage les mécanismes offerts par la Convention de Budapest. En 2020, 239 personnes ont été poursuivies pour des motifs liés à [les infractions qui touchent directement au système informatisé, à sa sécurité et aux données qui y sont stockées. […] 498 individus ont été poursuivis, dont plus de la moitié (261) était impliquée dans des affaires d'extorsion de fonds « à travers la menace de révélations ou d'imputations diffamatoires ». Une autre manière de nommer la pratique de la « sextorsion », ou chantage sexuel par voie électronique." READ MORE

Source: Seguri LATAM

Date: 8 Dec 2021

Colombia: Convenio sobre la Ciberdelincuencia: necesidad apremiante hacia 2022

"Adaptación y estandarización del Convenio sobre la Ciberdelincuencia a las nuevas acciones criminales que se puedan presentar en 2022. En esa misma línea, los escenarios pueden transformar al mismo tiempo que se cambian las tecnologías (Ortiz Ruiz, 2020) y la necesidad de incorporar en la ciberseguridad un nuevo diseño para poder contrarrestarlas puede necesitar la santa articulación en muchos frentes con grupos y tareas conjuntas para poder mitigar los nuevos ciberataques que se van a presentar. " READ MORE

Source: Bloomberg

Date: 7 Dec 2021

U.S. Efforts to Catch Cybercriminals Abroad Hinge on Extradition

"U.S. law enforcement's pursuit of global cybercrime is hampered by reliance on politically charged treaties governing extradition of suspected hackers. The U.S. lacks such treaties with Russia, China, and other nations from which such attacks have originated, preventing accountability for hackers harbored in their home country. Even when suspected cybercriminals are arrested in countries where such treaties are in place, law enforcement still struggles to bring cybercriminals to justice in U.S. courts due to years-long delays and legal challenges." READ MORE

Source: Meri Talk

Date: 10 Dec 2021

United States: Cybercrime Metrics Bill Clears Senate, House Judiciary

''The Better Cybercrime Metrics Act – legislation that aims to improve cybercrime data collection and give Federal law enforcement more tools to stop online crime – was approved this week by the Senate via unanimous consent, and by the House Judiciary Committee via voice vote. The bipartisan bill introduced earlier this year will "improve data collection on cybercrimes, giving law enforcement and policy makers more tools to understand the size and scope of cybercrime in the United States." READ MORE

Source: ZdNET

Date: 15 Dec 2021

US and Australia enter CLOUD Act agreement for cross-border access to electronic evidence

"Australia and the United States have entered into a landmark CLOUD Act agreement to bolster efforts in preventing serious organised crime, terrorism, ransomware attacks, critical infrastructure sabotage, and child sexual abuse. The Clarifying Lawful Overseas Use of Data Act, known as the CLOUD Act, is a US legal instrument that allows for law enforcement to access data across borders.." […] The CLOUD Act agreement comes off the heels of Australia announcing various initiatives in recent months to prevent crime. In December alone, Australia has announced the Online Safety Youth Advisory Council, passed "Magnitsky-style" and Critical Infrastructure cyber attack laws, commenced work on electronic surveillance law reforms, and proposed anti-trolling laws. The Australian government also started work on a new ransomware plan back in October. '' READ MORE

Source: Council of Europe

Date: 10 Dec 2021

GLACY+: Support for Drafting Data Protection Legislation in Vanuatu – Introductory workshop

''The workshop was the first in a process to support Vanuatu to harmonise its domestic legislation on data protection and privacy with international standards in the area, including Convention 108+ and the Budapest Convention on Cybercrime. At the end of the process, it is expected that Vanuatu will be able to present a data protection and privacy bill in line with international standards to the National Assembly, potentially at the November 2022 session. If adopted, it would be the first data protection legal framework in Vanuatu." READ MORE

Source: European Council

Date: 3 Dec 2021

Strengthening EU-wide cybersecurity and resilience – Council agrees its position

"Today, the Council agreed on its position ('general approach') on measures for a high common level of cybersecurity across the EU, to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole. Once adopted, the new directive, called 'NIS2', will replace the current directive on security of network and information systems (the NIS directive). […] The revised directive aims to remove divergences in cybersecurity requirements and in implementation of cybersecurity measures in different member states. To achieve this, it sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each member state. It updates the list of sectors and activities subject to cybersecurity obligations, and provides for remedies and sanctions to ensure enforcement.'' READ MORE

Source: European Commission

Date: 9 Dec 2021

The Commission proposes to extend the list of 'EU crimes' to hate speech and hate crime

"Today, the European Commission is presenting an initiative to extend the list of 'EU crimes' to hate speech and hate crime, as announced by President von der Leyen in her 2020 State of the Union speech. […] Common EU action is needed to tackle this EU-wide challenge. However, currently there is no legal basis to criminalise hate speech and hate crime at EU level. The existing list of EU crimes in the Treaty on the Functioning of the European Union (TFEU) needs to be extended to ensure minimum common rules on how to define criminal offences and sanctions applicable in all EU Member States." READ MORE

Source: Reuters

Date: 15 Dec 2021

UK lawmakers call for tougher crackdown on online scammers, cyberflashing

"Google, Facebook and other online services should be held legally accountable for advertisements on their platforms in order to prevent fraudsters scamming millions of consumers, a cross-party group of British lawmakers has said. Britain has proposed a landmark online safety law to punish abuses such as child pornography, racism and violence against women, but a joint committee of lawmakers drawn from both houses of parliament said on Tuesday it should go a step further to cover paid-for adverts." READ MORE

Source: Europol

Date: 13 Dec 2021

Arrest in Romania of a ransomware affiliate scavenging for sensitive data

"The criminal is suspected of having compromised the network of a large Romanian IT company delivering services to clients in the retail, energy and utilities sectors.

He is then believed to have deployed ransomware and stolen sensitive data from the IT company's clients located in Romania and abroad, before encrypting their files. The information stolen included the companies' financial information, personal information about employees, customers' details and other important documents. The suspect would then ask for a sizeable ransom payment in cryptocurrency, threatening to leak the stolen data on cybercrime forums should his demands not be met." READ MORE

RELATED ARTICLE:

Info Security, Police Arrest Suspected Ransomware Actor in Romania, 14 December 2021

Latest reports

- Cyber Pop-up, What we can learn from the most Alarming 2021 Breaches so far, 3 December 2021
- FindStack, La liste ultime des statistiques de piratage pour 2022, 5 December 2021
- EUROPOL, SIRIUS EU Digital Evidence Situation Report (updated), 6 December 2021
- Hiscox, Informe de Ciberpreparación de Hiscox 2021. No dejes tu ciberseguridad en manos del azar, 7 December 2021
- Security Boulevard, The Evolving Technology of Cybercrime, 8 December 2021
- Cybercrime Magazine, Top 30 Cybersecurity Experts You Should Follow In 2022, 8 December 2021
- European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Third Progress Report on the implementation of the EU Security Union Strategy, 8 December 2021
- Group-IB, HI-TECH CRIME TRENDS 2021/2022, 9 December 2021
- Mastercard, El desafío de la ciberseguridad en América Latina y el Caribe, 9 December 2021
- Brickmans Law, Electronic And Digital Evidence Admissibility Of E-signatures In Nigeria: Limits, Burdens And Opportunity, 9 December 2021
- Security Brief, New Zealand, An exclusive look at the NZ NCSC cyber crime report, 13 December 2021
- Alliance of Digitql Builders (AODB), [Dossier spécial Cybercriminalité] Une cybersécurité made in France, 13 December 2021
- Check Point Research, Threat Intelligence report, 13 December 2021
- ENISA, Securing Machine Learning Algorithms, 14 December 2021

Upcoming events

- 13-17 December, C-PROC/INTERPOL/ASIA & PACIFIC region, (*hybrid*), Cyber-enabled fraud training, GLACY+
- 14 December, C-PROC/INTERPOL/MEDITERRANEAN region, (*online*), Data protection and cybercrime, GLACY+
- 14-16 December, C-PROC/PANAMA, (*online*), Advisory workshop on the streamlining of procedures for MLA enhanced by the 2nd Additional Protocol related to cybercrime and electronic evidence combined with Specialized course on international cooperation, GLACY+
- 15 December, C-PROC, Meeting of the working group on e-learning training platform, C-PROC
- 16 December, C-PROC, *(online),* Working Group of the 24/7 Network under the Medicrime Convention, C-PROC
- 17 December, C-PROC/EAP countries, (*online*), IV Steering Committee, CyberEast
- 20-24 December, C-PROC/ARMENIA, (*in-person*), ECTEG Course on Network Investigations for Armenian counterparts (led by OSCE), CyberEast
- 21 December, C-PROC/ECUADOR, *(online),* Consultation roundtable on the draft regulation in the application of data protection law, GLACY+

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of December have been rescheduled to a later date.

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