# Cybercrime Digest

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

1 – 15 December 2020

*Source: Romania-Insider*

*Date:10 Dec 2020*

## Bucharest to host EU's new cybersecurity center

“Bucharest will host the European Cybersecurity Industrial, Technology, and Research Competence Centre, which is meant to improve cyber-resilience and support cybersecurity research across the EU.[…]Bucharest was chosen from a list of cities that included Brussels, Munich, Warsaw, Vilnius, Luxembourg, and León (Spain).[…] In its application to host the center, Romania highlighted the "broad pool of IT&C specialists due to its excellent education system in this area" and that it ranks third in the EU statistics referring to the women ICT specialists.[…] Bucharest also hosts the Cybercrime Program Office of the Council of Europe (C-PROC).This assists countries in strengthening their legal systems capacity to respond to the challenges posed by cybercrime.” READ MORE

RELATED ARTICLES

Council of Europe, European Cybersecurity Competence Center to be located in Bucharest, 11 December 2020

*Source: Council of Europe*

*Date: 8-9 Dec 2020*

## Eurojust and the Council of Europe hold a Joint Workshop on International Cooperation

“Two days, two institutions, two sets of countries – Eurojust and the Council of Europe joined forces in what becomes a yearly tradition, holding a Joint Workshop on International Cooperation in Cybercrime and Electronic Evidence on 8-9 December 2020 in a fully virtual environment. […] the event offered the opportunity to discuss the tools and projects at Eurojust contributing to international cooperation on cybercrime and electronic evidence, and to present and discuss the Second Additional Protocol to the Budapest Convention on Cybercrime.”READ MORE

*Source: INTERPOL*

*Date: 1 Dec 2020*

## INTERPOL: Artificial Intelligence and law enforcement: challenges and opportunities

“The disruption of AI-controlled systems, AI-authored fake news, and the use of driverless systems as weapons were identified as probable AI-enabled future crimes during the INTERPOL-UNICRI Global Meeting on Artificial Intelligence for Law Enforcement. […] There was a consensus that a more data-driven and scientific approach to criminal investigations would be crucial in tackling AI-related threats. These observations will be taken into account in the development of a “Responsible AI Innovation Toolkit for Law Enforcement”.” READ MORE

*Source: Council of Europe*

*Date: 11 Dec 2020*

## United Kingdom makes a further voluntary contribution to the new Octopus Project

“The United Kingdom has made a further voluntary contribution to the new Octopus project, amounting to UK Pounds 100,000. The new project aims to support the implementation of the Budapest Convention on Cybercrime (CETS 185), its Protocols and related standards through the Cybercrime Convention Committee (T-CY) and the Cybercrime Programme Office (C-PROC). The United Kingdom is a Party to the Budapest Convention since 2011.” READ MORE

*Source: European Parliament*

*Date: 7 Dec 2020*

## Detecting online child sexual abuse requires strong safeguards

"The Civil Liberties Committee wants safeguards to ensure that tools used to detect and remove online child sexual abuse respect people's fundamental rights. The proposed regulation will provide for limited and temporary changes to the rules governing the privacy of electronic communications so that over the top ("OTT") communication interpersonal services, such as web messaging, voice over Internet Protocol (VoIP), chat and web-based email services, can continue to detect, report and remove child sexual abuse online on a voluntary basis." READ MORE

*Source: Law Society Gazette Ireland*

*Date: 16 Dec 2020*

## Lanzarote Convention is to be ratified by Ireland

"The Government has approved the ratification of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention). The Convention is a Council of Europe instrument to prevent and combat sexual exploitation and sexual abuse of children, to protect the rights of child victims of sexual exploitation and sexual abuse, and to promote national and international co-operation against such conduct. It is a significant, international, legal instrument in protecting children. Justice minister Helen McEntee said this morning: "Sexual exploitation and sexual abuse has devastating consequences for child victims, their families and as society as a whole. "Protecting children is a key priority for this Government, and ratifying the Convention delivers an important message that Ireland is committed to the fight against these reprehensible crimes, which target some of the most vulnerable in our society." READ MORE

*Source:INTERPOL*

*Date: 9 Dec 2020*

## INTERPOL: More than 20,000 arrests in year-long global crackdown on phone and Internet scams

"A year-long investigative clampdown on criminal networks coordinated by INTERPOL has demonstrated the scale of phone and online frauds worldwide. Codenamed First Light, the operation officially concluded in November with the following results: 10,380 locations raided, 21,549 operators, fraudsters and money launderers arrested, 310 bank accounts frozen, USD 153 973 709 worth of illicit funds intercepted. This latest edition of Operation First Light marked the first time law enforcement has coordinated with INTERPOL on a global scale to combat telecoms fraud, with operations taking place on every continent." READ MORE

*Source:Europol*

*Date: 2 Dec  2020*

## Europol: 422 arrested and 4031 money mules identified in global crackdown money laundering

The "law enforcement authorities from 26 countries and Europol announced the results of the European Money Mule Action 'EMMA 6', a worldwide operation against money mule schemes. Between September and November 2020, EMMA 6 was carried out for the sixth consecutive year with the support of the European Banking Federation (EBF), FinTech FinCrime Exchange, INTERPOL and Western Union. During the span of the operation, 1 529 criminal investigations were initiated. With the support of the private sector including more than 500 banks and financial institutions, 4 942 fraudulent money mule transactions were identified, preventing a total loss estimated at €33.5 million." READ MORE

*Source: Council of Europe*

*Date: 14 Dec 2020*

## Freedom of Expression and Data Privacy standards promoted in the Philippines

"The Philippines - UN Human Rights Summit hosted Council of Europe's head of Information Society Patrick Penninckx outlining The Global Landscape of Freedom of Expression on the Internet in a webinar on "Freedom of Expression and Data Privacy on Social Media" webcasted on 10 December. The speaker highlighted the challenges of the new digital environment and the Covid-19 pandemic on freedom of expression as well as explained the protection provided by Convention 108 and its additional protocol, and the Convention of Cybercrime, areas of ongoing cooperation between the Philippines and the Council of Europe. Organised by the Ministry of Justice of the Philippines, the webinar features also talks on rights and remedies for freedom of expression on social media in the Philippine legal framework, electronic evidence and cyber libel, data privacy on social media and cybersecurity measures. The impetus for the event was brought by the impact Internet has made on many aspects of human lives including the way we communicate with friends and family, gather and share information, and express opinions. Covid-19 has accelerated the digital transformation. The increasingly captivity to internet and social media raises growing concerns on digital etiquette, cyber bullying and cyber libel." READ MORE

*Source: Council of Europe*

*Date: 9 Dec 2020*

## Work continues on the development of Standard Operating Procedures (SOPs) in Lebanon

"In the framework of the CyberSouth Project, the Second online national meeting on the Development of Standard Operating Procedures (SOPs) and Toolkit for First Responders on Cybercrime Investigations and E-evidence was held with Lebanon […]. The goal of this meeting was to discuss with the representatives of the Internal Security Forces the assessment of the draft SOPs on e-evidence. Lebanese representatives presented existing practices and standards, and interacted with international experts on potential gaps and recommendations on how to align them with national legislation, international best practices and investigation techniques involved in the process." READ MORE

*Source: The Wall Street Journal*

*Date: 13 Dec 2020*

## U.S. Agencies Hacked in Foreign Cyber Espionage Campaign Linked to Russia

"Multiple federal government agencies, including the U.S. Treasury and Commerce departments, have had some of their computer systems breached as part of a widespread global cyber espionage campaign believed to be the work of the Russian government. […] The hacking operation exposed as many as hundreds of thousands of government and corporate networks to potential risk […] Sophisticated hackers increasingly have sought to rely on so-called supply-chain attacks in which they can harness a vulnerability in a common product or service used widely across the internet to rapidly hack scores of victims before the compromises are detected." READ MORE

RELATED ARTICLES

CNN, US officials scramble to deal with suspected Russian hack of government agencies, 14 December 2020

*Source: Council of Europe*

*Date: 25-27 Nov 2020*

## Virtual Workshop on Data Protection and Global Policing Capabilities implemented by INTERPOL

During the period of 25 - 27 November 2020, the Global Action on Cybercrime Extended Project (GLACY+) organised online the Regional Workshop on Data Protection and Global Policing Capabilities for 51 representatives from police, judiciary and data protection communities from Chile, Costa Rica and Paraguay. As data protection is essential in the international police to police cooperation and global sharing of police information and intelligence, there is an increasing demand to strengthen the capabilities and tools for data exchange under the data protection framework." READ MORE

*Source: Al Dia Chile*

*Date:1 Dec 2020*

## Chile: Comisión de Seguridad Ciudadana despacha proyecto sobre delitos informáticos

"El proyecto que deroga la ley vigente sobre la materia, con el objeto de adecuar la normativa nacional al Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como Convenio de Budapest, fue derivada ahora a la Comisión de Ciencias y Tecnología. […] De dicho modo, se tipifica una serie de conductas […], considerando los cada vez más recurrentes ataques a la integridad de los sistemas informáticos a nivel mundial, así como el acceso e interceptación ilícitos; el ataque a la integridad de los datos informáticos; la falsificación informática; el fraude informático; y el abuso de dispositivos." READ MORE

*Source: Câmara dos Deputados Brasil*

*Date: 2 Dec 2020*

## Brazil: Projeto altera legislação penal para ampliar punição de crime cibernético

"O texto altera o Código Penal, que hoje prevê detenção de 3 meses a 1 ano, e multa, para os crimes cibernéticos. [...] Para Luizão Goulart, a pena atual é branda diante do avanço dos crimes cibernéticos. Ele lembra que esse tipo de crime cresceu durante a pandemia. Exemplos recentes foram a invasão aos computadores do Superior Tribunal de Justiça (STJ) e do Tribunal Superior Eleitoral (TSE), esta ocorrida durante o 1º turno da eleição municipal. [...] O projeto prevê ainda prisão de 6 a 12 anos se da invasão resultar ao dono do equipamento indisponibilidade de dados ou informações" READ MORE

*Source: Asamblea Legislativa El Salvador*

*Date: 1 Dec 2020*

## El Salvador: Comisión de Seguridad continúa estudio de reformas a Ley contra Delitos Informáticos

"La Comisión de Seguridad Pública y Combate a la Narcoactividad continúa recabando insumos para aprobar reformas a la Ley Especial contra los Delitos Informáticos y Conexos. La ley vigente, que fue aprobada por la Asamblea Legislativa en febrero de 2016, no ha sufrido enmiendas, por lo que los diputados consideran oportuno que se haga un estudio de su impacto, dado que, a través de tecnologías informáticas, como redes sociales, se puede cometer delitos. Y es que en la misma legislación, en sus considerandos, se reconoce que muchos de las actividades delincuenciales, a través de las diferentes herramientas tecnológicas, no están totalmente reguladas; en ese sentido, los legisladores han mencionado la creación de medios informativos digitales o espacios de noticias en los que se comete delitos relativos a la dignidad de las personas […]." READ MORE

*Source: Lexology*

*Date: 8 Dec 2020*

## South Africa: Cybercrimes Bill to be submitted to the president for signature

"On 2 December 2020, the South African Parliament passed the Cybercrimes Bill ("Bill"), which will be submitted to the South African President for assent. The Bill creates many new offences with the majority of these being related to data, messages, computers, and networks involving hacking, the unlawful interception of data, ransomware attacks, cyber forgery and uttering, and cyber extortion. The Bill also grants law enforcement extensive powers to investigate, search, access and seize various articles, such as computers, databases or networks." READ MORE

*Source: Europol*

*Date: 11 Dec 2020*

## Finnish Customs take down Sipulimarket on the dark web with Europol support

"Drugs and other illegal commodities were sold in large quantities on Sipulimarket which had been operating on the The Onion Router (Tor) network since 2019. […] Europol supported the Finnish Customs by providing operational support and technical expertise, including hosting the seizure banner." READ MORE

*Source: Asia Nikkei*

*Date: 14 Dec 2020*

## Indian IT companies step up fight against cyberattacks

"India's leading IT services companies are ramping up cybersecurity measures to address the increasing threat of cyberattacks across sectors and regions. […] Indian IT companies are also citing the increasing intensity of cyberattacks as well as the need to secure larger areas including remote workplaces amid the pandemic, as reasons for strengthening their countermeasures." READ MORE

*Source: IT News Africa*

*Date: 8 Dec 2020*

## How COVID-19 has Changed the Shape of African Cybersecurity

"This year, respondents were even more concerned about cybercrime compared with 2019 […]. The 2020 KnowBe4 African Report – which collated insights from across South Africa, Kenya, Nigeria, Ghana, Egypt, Morocco, Mauritius and Botswana – found that attitudes and behaviours had shifted as a result of the pandemic, but problem pockets of risk remain that need to be addressed in order to ensure both business and individual security. […] Email security is one of the biggest threats facing the average user, both at work and at home, and it is one of the most common communication methods – nearly 87% use email for work, closely followed by WhatsApp at 85%." READ MORE

*Source: ZD Net*

*Date: 10 Dec 2020*

## Hackers are selling more than 85,000 MySQL databases on a dark web portal

"More than 85,000 MySQL databases are currently on sale on a dark web portal for a price of only $550/database. […] The price for recovering or buying a stolen database must be paid in bitcoin. The actual price has varied across the year as the BTC/USD exchange rate fluctuated but has usually remained centered around a $500 figure for each site, regardless of the content they included. This suggests that both the DB intrusions and the ransom/auction web pages are automated […]" READ MORE

*Source: ZD Net*

*Date: 1 Dec 2020*

## Les cyberattaques qui ont marqué l'année 2020

“La pandémie n'a pas empêché les cybercriminels de multiplier les piratages au cours de cette année. Retour sur les attaques qui ont marqué l'année 2020. […] Des recherches suggèrent que le travail à distance est devenu la source de 20 % des incidents de cybersécurité, que les rançongiciels sont en augmentation, et que nous devons encore intégrer le fait que "123456" n'est pas un mot de passe adéquat.” READ MORE

*Source: Hypertext*

*Date: 1 Dec 2020*

## Crypto, skimmers and extortion prime targets for cybercriminals in 2021

“Cybercrime has been a constant fixture throughout 2020 and that won’t change when the calendar flips to 2021. […] One of the more concerning predictions is a rise in extortion tied to ransomware attacks. […]In order to execute these extortion attempts, Kaspersky predicts that ransomware gangs will use zero-day exploits more frequently throughout 2021.” READ MORE

## Latest reports

- Council of Europe, Towards regulation of AI systems, 14 Dec 2020
- Eurojust, Challenges and best practices from Eurojust's casework in the area of cybercrime, November 2020
- European Parliament, Report for a Regulation on European Production and Preservation Orders for electronic information in criminal proceedings, 11 Dec 2020
- Europan Union Agency for Fundamental Rights (FRA), Getting the future right – Artificial intelligence and fundamental rights, 14 Dec 2020
- ENISA, Updated ENISA 5G Threat Landscape Report to Enhance 5G Security, 14 December 2020
- ENISA, Driving the Global Ecosystem of Incident Response Capabilities: New Studies Now Available, 10 December 2020
- ENISA, Focus on National Cybersecurity Capabilities: New Self-Assessment Framework to Empower EU Member States, 7 December 2020
- APWG, Phishing Activity Trends Report 3rdQuarter, November 2020

## Upcoming events

- 14-16 December, C-PROC/Ukraine, (on-line), Effective access to data exercise and development of standard procedures between LEA/ISPs, CyberEast
- 14-16 December, C-PROC/Gambia, (on-line), Support for drafting the Data Protection Law, in collaboration with the Data Protection Unit of the Council of Europe, GLACY+
- 17 December, C-PROC, Webinar on CyberSecurity and Human Rights, led by CyberSecurity EAST project, CyberEast
- 22 December, C-PROC/Kosovo*, (on-line), Meeting on the assessment of the collection and investigation/ handling of electronic evidence, iPROCEEDS-2

*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. News are selected by relevance to the current areas of interest to C-PROC and do 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