Cybercrime Digest

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

1 – 15 April 2022

Source: Council of Europe

Date: 1 April 2022

Register before 19 April! International conference and opening for signature of the 2nd Additional Protocol to the Convention on Cybercrime

Following almost four years of negotiations (September 2017 – May 2021) and formal approval on 17 November 2021, the 2nd Additional Protocol to the Budapest Convention on Cybercrime is now to be opened for signature by the Parties to the Convention at the Council of Europe in Strasbourg, France, in the framework of an international conference on Enhanced co–operation and disclosure of electronic evidence on 12-13 May in Strasbourg. The meeting will be opened by Marija Pejčinović Burić, Secretary General of the Council of Europe, and the Minister of Justice of Italy, and will be followed by interventions by ministers and other senior officials from Parties to the Convention. READ MORE

Source: Council of Europe

Date: 4 April 2022

Ecuador invited to join the Budapest Convention on Cybercrime

Ecuador was invited on 30 March 2022 to accede to the Budapest Convention on Cybercrime. Thus, 81 States are now either Parties (66), or have signed it or been invited to accede (15). The authorities of Ecuador have been cooperating with the Council of Europe in cybercrime matters on multiple occasions, starting in 2008, when the Organisation of American States and the Council of Europe co-organised a regional workshop on cybercrime for countries of Latin America held in Colombia. In 2020/2021, this led to reforms of criminal law that brought domestic legislation broadly in line with the substantive criminal law articles of the Budapest Convention on Cybercrime. READ MORE

Source: European Council and Council of the EU

Date: 5 April 2022

Access to e-evidence: Council authorises member states to sign international agreement

“The Council today adopted a decision authorising member state to sign, in the interest of the EU, the second additional protocol to the convention on cybercrime of the Council of Europe (Budapest convention). This protocol will improve cross-border access to electronic evidence to be used in criminal proceedings. It will contribute to the fight against cybercrime and other forms of crime at global level by simplifying cooperation between member states and third-countries, while ensuring a high level of protection for individuals and the compliance with EU data protection standards. […] This text will complement the EU framework on access to e-evidence currently being discussed by the EU institutions. Its advantage is its potential to be of application across the globe. Currently, 66 countries are party to the Budapest convention, including 26 member states.” READ MORE

Source: Council of Europe

Date: 8 April 2022

Council of Europe HELP online Course on Cybercrime and Electronic Evidence

"Cybercrime and other crimes involving electronic evidence affect the right to private life of hundreds of millions of individuals whose personal data are stolen; attack the dignity and the integrity of individuals; are a threat to the freedom of expression, public security but also democratic stability. An effective criminal justice response is needed in order to protect societies against cybercrime while also protecting individuals' fundamental human rights. The new HELP course is aiming to introduce the basic concepts related to cybercrime and electronic evidence by making an overview of the challenges in investigating cybercrime, as well as the difficulties in collecting and handling of electronic evidence." READ MORE

Source: Euronews

Date: 6 April 2022

How digital evidence of war crimes in Ukraine is being collected, verified and preserved

"As international outrage grows over the killings of civilians in Ukraine, human rights defenders are working around the clock to collect, verify and preserve digital evidence of the attacks - to someday hold those responsible to account. […] Because of its graphic nature, the content can be quickly taken down by social media platforms whose policies it violates. Meta, which owns Facebook and Instagram, said this week it was "exploring ways to preserve this type and other types of content when we remove it," specifically in relation to the war in Ukraine. Witness and other NGOs have for years been pressuring social media companies to create repositories for evidence surrounding possible war crimes, to ensure it remains accessible to human rights researchers and investigators." READ MORE

RELATED ARTICLE:

Cyberscoop, Russian attempts to phish Ukrainian targets with 'war crimes' lures unsuccessful so far, official says, 5 April 2022

Source: Council of Europe

Date: 8 April 2022

Child self-generated sexual images and videos: new report provides guidance to governments

"Addressing challenges raised by the significant increase and exploitation of child self-generated sexual images and videos is the focus of the new monitoring report presented by the Council of Europe's Lanzarote Committee in Rome. The report covers 43 European states Parties to the Lanzarote Convention, and highlights ways to improve their legal framework, prevent this particular form of sexual exploitation of children, investigate and prosecute it and enhance the victims' identification and protection. For the first time, children directly participated in the monitoring process: the monitoring report reflects views of more than 300 children from ten European states on the challenges stemming from the self-generation of sexual material." READ MORE

Source: ZDNet

Date: 6 April 2022

US Justice Department shuts down Russian dark web marketplace Hydra

"The US Department of Justice (DOJ) has shut down Hydra Market, one of the world's largest darknet marketplaces. On Tuesday, the DOJ and German federal police seized Hydra's servers and cryptocurrency wallets containing $25 million worth of bitcoin. Hydra was an online criminal marketplace where primarily Russian users bought and sold illicit goods and services, including illegal drugs, stolen financial information, fraudulent identification documents, and money laundering and mixing services. […] In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace has received approximately $5.2 billion in cryptocurrency, the DOJ said." READ MORE

RELATED ARTICLES:

U.S. Department of Justice, Justice Department Investigation Leads To Shutdown Of Largest Online Darknet Marketplace, 5 April 2022

BBC News, Hydra: How German police dismantled Russian darknet site, 6 April 2022

Zeit Online, Deutsche Ermittler schalten illegalen Marktplatz im Darknet ab, 5 April 2022

Source: Techcrunch

Date: 5 April 2022

Europe's top court sharpens guidance on data retention for combating serious crime

"A ruling by the European Union's top court has reaffirmed that national law cannot rely on a claim of combating serious crime to deviate from the prohibition in EU law on general and indiscriminate collection of electronic comms data. Although the court has signposted some targeted exceptions it suggests may be permissible for gathering digital evidence in bulk to fight serious crime, such as by targeting places with a high instance of crime or a high volume of visitors (such as airports), or other locations which house critical infrastructure." READ MORE

Source: ICANN

Date: 11 April 2022

ICANN Responds to Call for Evidence on EU Toolbox Against Counterfeiting

"The Internet Corporation for Assigned Names and Numbers (ICANN) announced today that on 6 April 2022 the ICANN organization (ICANN org) provided feedback to the Call for Evidence launched by the European Commission (EC) on the European Union's (EU) Toolbox Against Counterfeiting. The EU Toolbox Against Counterfeiting is part of the EC's Intellectual Property (IP) Action Plan. The initiative seeks to step up the fight against counterfeiting by clarifying the roles and responsibilities of rights holders, intermediaries, and public authorities with respect to mutual cooperation and data sharing. It is especially aimed at enhancing cooperation between parties. Intermediaries are identified as social media platforms, the domain name ecosystem, payment services, and the transport and logistics industries." READ MORE

Source: Europol

Date: 12 April 2022

One of the world's biggest hacker forums taken down

"The illegal marketplace 'RaidForums' has been shut down and its infrastructure seized as a result of Operation TOURNIQUET, a complex law enforcement effort coordinated by Europol to support independent investigations of the United States, United Kingdom, Sweden, Portugal, and Romania. The forum's administrator and two of his accomplices have also been arrested. Launched in 2015, RaidForums was considered one of the world's biggest hacking forums with a community of over half a million users. This marketplace had made a name for itself by selling access to high-profile database leaks belonging to a number of US corporations across different industries. These contained information for millions of credit cards, bank account numbers and routing information, and the usernames and associated passwords needed to access online accounts." READ MORE

RELATED ARTICLE:

U.S. Department of Justice, United States Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator, 12 April 2022

Source: Council of Europe

Date: 5 April 2022

GLACY+/CyberSouth: Guide for law enforcement training strategies on cybercrime and electronic evidence published

"On 5 April, the Cybercrime Programme Office of the Council of Europe (C-PROC) and the INTERPOL Cybercrime Directorate published a Guide for Developing Law Enforcement Training Strategies on Cybercrime and Electronic Evidence. The guide was prepared under the Global Action on Cybercrime Extended (GLACY+) and the CyberSouth joint projects of the European Union and the Council of Europe to help LEAs coordinate their efforts for capability development." READ MORE

Source: Europol

Date: 8 April 2022

Tackling hate crime across Europe: second joint action day targets over 170 individuals

"The second EU-wide joint action day against hate crime, supported by Europol's European Counter Terrorism Centre (ECTC) and led by France, targeted racist and xenophobic hate speech and other hate crimes on the internet and in the real world. The operation took place in 11 countries. On the action day, 7 April 2022, law enforcement authorities raided multiple locations across Europe and targeted 176 individuals in relation to offences such as dissemination of racist and xenophobic hate speech, calls to violence, and incitement to commit offences. For example in Austria, authorities carried out 12 house searches, interrogated 8 individuals and seized electronic devices, mobile phones, weapons and propaganda material. Meanwhile, Spanish authorities targeted five individuals and arrested four of them for disseminating hate speech online." READ MORE

Source: United States Department of Justice

Date: 6 April 2022

Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate

"The Justice Department today announced a court-authorized operation, conducted in March 2022, to disrupt a two-tiered global botnet of thousands of infected network hardware devices under the control of a threat actor known to security researchers as Sandworm, which the U.S. government has previously attributed to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (the GRU). The operation copied and removed malware from vulnerable internet-connected firewall devices that Sandworm used for command and control (C2) of the underlying botnet. Although the operation did not involve access to the Sandworm malware on the thousands of underlying victim devices worldwide, referred to as "bots," the disabling of the C2 mechanism severed those bots from the Sandworm C2 devices' control." READ MORE

RELATED ARTICLE:

Cyberscoop, DOJ's Sandworm operation raises questions about how far feds can go to disarm botnets, 8 April 2022

Krebsonsecurity.com, Actions Target Russian Govt. Botnet, Hydra Dark Market, 7 April 2022

Source: Council of Europe

Date: 6 April 2022

Tackling the risks for democracy of digital political campaigning: Council of Europe issues guidelines

"The Council of Europe has issued a set of guidelines to its 46 member states to address the challenges to the fairness and legitimacy of electoral processes created by new digital political communication techniques. These challenges include the possible abusive use of microtargeting, personal data, bots and algorithms, as well as disinformation campaigns. The guidelines, adopted by the Committee of Ministers in a Recommendation, establish a number of principles to ensure the transparency of online electoral communication and expenditure, prevent manipulation of the electorate and ensure that political parties and candidates can compete on equal terms. They also tackle issues such as data protection, content regulation and media coverage of campaigns." READ MORE

Source: Journal du Cameroun

Date: 5 April 2022

Cameroun : l'Assemblée nationale adopte une loi sur la cybercriminalité

"Les parlementaires se sont penchés sur le sujet vendredi 01 avril 2022. Ils en ont profité pour faire passer un texte œuvrant pour promouvoir la cybersécurité. Le nouveau texte de loi a été adopté en plénière à l'Assemblée nationale. Une séance présidée par la vice-présidente de la Chambre l'honorable Mary Muyali Meboka. Le texte de loi fait état de manœuvres qui visent à lutter contre la cybercriminalité afin de protéger tant les internautes que l'ensemble de la société. Ainsi, les parlementaires ont adopté la loi N°2012/PJL/AN autorisant le chef de l'Etat à procéder à l'ascension du Cameroun à la Convention de Budapest. Une convention adoptée le 23 novembre 2001 à Budapest en Hongrie." READ MORE

RELATED ARTICLE:

ITWEB AFRICA, Cameroon hoping to join Budapest Convention to curb cybercrime, 4 April 2022

Source: ECOWAS Community Court of Justice

Date: 1 April 2022

Court orders Nigeria to align its cybercrime law with its international obligations

"The ECOWAS Court of Justice has ordered the Republic of Nigeria to amend Section 24 of its Cybercrime (Prohibition, Prevention, etc) Act of 2015 in order to ensure conformity with the country's obligations under the African Charter on Human and Peoples' Rights (ACHPR) and the International Covenant on Civil and Political Rights (ICCPR). Delivering judgement on Friday, 25th March 2022 during the Courts sitting in Accra in a case filed by the Registered Trustees of the Socio-Economic and Accountability Project (SERPA), a Non-Governmental Organisation, Justice Keikura Bangura who read the decision of the Court, said that the Section was not in conformity with Articles 9 of the ACHPR and 19 of the ICCPR to which the country is signatory." READ MORE

RELATED ARTICLE:

The Record, ECOWAS Court orders Nigeria to amend Cybercrime Law, 1 April 2022

Source: Interpol

Date: 5 April 2022

Financial crime: South African fraud gang dismantled

"A fraud gang suspected of swindling a US-based company out of some EUR 455,000 has been taken down in raids across Johannesburg led by investigators from the Hawks Serious Commercial Crimes Unit and US Secret Service agents, and supported by INTERPOL. With investigations on-going, the operation led to the arrest of seven people allegedly linked to a Nigerian organized crime syndicate that specializes in online fraud. The suspects allegedly bought luxury vehicles with the proceeds of their crimes." READ MORE

Source: Canadian Lawyers

Date: 12 April 2022

Canada and U.S. negotiating cross-border data-sharing agreement

"Canada and the U.S. recently agreed to negotiate a bilateral agreement to allow their respective law-enforcement agencies easier access to electronic data stored on the other side of the border. The U.S. is forging agreements with foreign governments under its Clarifying Lawful Overseas Use of Data (CLOUD) Act and has done so with Australia and the UK. The U.S. enacted the CLOUD Act in 2018. To access U.S.-housed data, Canadian law enforcement must use a Mutual Legal Assistance Treaty (MLAT). The use of these treaties has "expanded dramatically" in recent years, which has led to strained resources and slower response times, said the U.S. Department of Justice (DOJ)." READ MORE

Source: Universidad de Chile

Date: 6 April 2022

El principio de cooperación internacional en materia de ciberseguridad en el derecho chileno

"Después de su aprobación por el Congreso y la consecuente ratificación, Chile promulgó en abril de 2017 (D.S. 83/20171) el Convenio sobre la Ciberdelincuencia, adoptado en Budapest en 2001. Su publicación se realizó el 28 de agosto de 2017. Al hacerse parte, se plantea la pregunta sobre el alcance y la eficacia del principio de cooperación internacional y su relación con la obligación de legislar sobre materias de ciberseguridad." READ MORE

Source: Bleeping Computer

Date: 14 April 2022

FBI: Payment app users targeted in social engineering attacks

"Cybercriminals are attempting to trick American users of digital payment apps into making instant money transfers in social engineering attacks using text messages with fake bank fraud alerts. The warning, published by the Federal Bureau of Investigation as a public service announcement on Thursday, says the attackers will call victims who respond to their phishing messages from phone numbers spoofing the banks' legitimate 1-800 support number." READ MORE

Source: OGDI

Date: 10 April 2022

Los Delitos Informáticos en Guatemala

"En los últimos 20 años, el fenómeno de los ciberdelitos o cibercrimen como se le conocen en el mundo anglosajón, se encuentra presente en el País con un crecimiento exponencial que, en algún momento, explotará cuando toque fibras sensibles que dañarán intereses corporativos, gubernamentales o de alguna personalidad y es allí, cuando volverán la vista y tomarán las riendas de iniciativas y convenios internacionales que se han venido trabajando en diversas mesas técnicas desde el año 2008, encontrandose en un estado inerte y sin dar su fruto." READ MORE

Source: Cyberscoop

Date: 13 April 2022

DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii

"Federal agents in Honolulu last week "disrupted" an apparent cyberattack on an unnamed telecommunication company's servers associated with an underwater cable responsible for internet, cable service and cell connections in Hawaii and the region, the agency said in a statement Tuesday. Hawaii-based agents with Homeland Security Investigations, an arm of the Department of Homeland Security, received a tip from their mainland HSI counterparts that led to the disruption of a "significant breach involving a private company's servers associated with an undersea cable." The investigation revealed that "an international hacking group" was behind the attack, and "HSI agents and international law enforcement partners in several countries were able to make an arrest."" READ MORE

Source: BBC

Date: 13 April 2022

CPC: Criminal Procedure Identification Bill raises fears of surveillance in India

"A proposed new Indian law gives sweeping powers to law enforcement agencies to collect biometric data - a move that has sparked concerns over privacy. The Criminal Procedure (Identification) bill, which was passed in parliament last week, makes it compulsory for those arrested or detained to share sensitive data - like iris and retina scans. The police can retain this data for up to 75 years. The bill will now be sent to the president for his assent." READ MORE

Source: Atlantic Council

Date: 12 April 2022

The Internet 'Protection Bill' will hurt all Iranians, but the queer community will have the most to lose

"International human rights organizations and the United Nations are saying a lot about the repressive "Regulatory System for Cyberspace Services Bill"—widely referred to as the "Protection Bill"—currently under review by the Iranian parliament. However, not much light has been shed on one of the most marginalized groups that will suffer the most: Iran's LGBTQI community." READ MORE

Source: FinancialIT

Date:13 April 2022

Withsecure™ Cofounds Cyberspace Project to Counter Cyber Crime in Europe

"WithSecure™, formerly known as F-Secure Business, and 10 other European organizations have cofounded the CYBERSPACE project. The project is a 3-year initiative funded by the European Commission to support European law enforcement agencies and improve their capacity to investigate and counter cybercrime. […] The group aims to help organizations work together to compile and share information and intelligence related to cyber attacks and cyber crime. It also aims to develop new tools to help law enforcement and other defenders investigate and respond to attacks." READ MORE

Source: The Register

Date: 9 April 2022

Finnish govt websites knocked down as Ukraine President addresses MPs

“Cyberattacks took down Finnish government websites on Friday while Ukrainian President Volodymyr Zelenskyy addressed Finland's members of parliament (MPs). Denial-of-service (DoS) attacks hit Finland's ministries of Defense and Foreign Affairs' websites around noon local time. About an hour later, both government agencies tweeted that the websites were back up and running.” READ MORE

Latest reports

- Puromarketing, El robo de datos de clientes de Iberdrola y cómo el cibercrimen se ha convertido en una amenaza reputacional seria, 1 April 2022
- Digital Guardian, A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, 4 April 2022
- Security Brief Australia, The rise of cybercrime - Over $300 million lost to scams last year, 5 April 2022
- SciDevNet, L'Afrique a perdu 10% de son PIB en 2021 du fait de la cybercriminalité, 6 April 2022
- Atlas VPN, 60 Worrying Cybercrime Statistics & Facts [2022], 6 April 2022
- Mondaq, Switzerland: Cybersecurity Comparative Guide, 6 April 2022
- Web Tribunal, 54 Cybersecurity Statistics from 2022: Stay Safe in the New Decade, 6 April 2022
- Animalmx, ¡No Caigas en el Engano! Que es el Spoofing y como Identificar este Cibercrimen, 7 April 2022
- Wired, Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site, 7 April 2022
- Trusted Digital Forensics Expert Authors Book: Forensics Data Collections 2.0: The Guide for Defensible & Efficient Processes, 7 April 2022
- Info Security, Fraudsters Steal £58m in 2021 Via Remote Access Tools, 11 April 2022
- ASPI, Artificial intelligence: your questions answered, 11 April 2022
- Foundation for Media Alternatives, Year-end Cybercrime and Human Rights Report 2021, 11 April 2022
- WSR, 40+ Cybersecurity Statistics & Facts For 2022, 12 April 2022
- Splunk, Cybersécurité en 2022 : les Français restent optimistes face à l'explosion des attaques, 12 April 2022
- Cyberpeace Institute, Ukraine: timeline of cyberattacks on critical infrastructure and civilian objects, 13 April 2022
- Enisa: Coordinated Vulnerability Disclosure policies in the EU, 13 April 2022
- Modern Diplomacy, U.S- NATO role in the cyber conflict and Taiwan to confront China after the Ukraine war, 13 April 2022
- SoSafe: Human Risk Review 2022, 13 April 2022
- The Press Free, Rapport sur les marchés mondiaux des technologies de déception 2022 : le marché atteindra 4,2 milliards de dollars d'ici 2026, 14 April 2022
- BDM, Ransomwares en entreprise : chiffres clés et conseils pour s'en prémunir en 2022, 14 April 20220

Upcoming events

- 18-19 April, C-PROC/GEORGIA, (*in-person),* Workshop with Georgian authorities on cybercrime policies, CyberEast
- 19-20 April, C-PROC/CHILE, *(online),* Advisory mission on data protection legislation, GLACY+
- 22 April, C-PROC, *(online),* Working Group on undercover investigations and extension of searches -4th meeting, T-CY
- 27-29 April, C-PROC/COLOMBIA, *(hybrid),* Workshop on the universality of the Budapest Convention and the role of policy makers on cybercrime legislation, GLACY+, OCTOPUS
- 27 April (TBC), C-PROC/VANUATU, *(online),* Advisory mission on data protection legislation - debriefing session: policy drafting, GLACY+
- 27 April, C-PROC/FIJI, *(hybrid),* Series on workshops on the new cybercrime act and international standards for judges, GLACY+, OCTOPUS
- 28 April , C-PROC/APWG, *(online),* International Cooperation on Cybercrime Prevention, Investigation and Prosecution Using Emerging Technologies: challenges and opportunities, GLACY+
- 28 April, C-PROC/FIJI, *(hybrid),* Series on workshops on the new cybercrime act and international standards for prosecutors, police & FIU, GLACY+, OCTOPUS
- 29 April, C-PROC/FIJI, *(hybrid),* Series on workshops on the new cybercrime act and international standards for service providers, GLACY+,OCTOPUS
- April, C-PROC, (*online*), Revision and publication of a series of OCSEA country profiles into the Octopus platform, OCTOPUS
- April-May, C-PROC, *(online),* Review of 2017 Study on Cooperation with Multinational Service Providers, CyberEast
- April-May 2022, C-PROC, (*online*), Translation of the Electronic Evidence Guide 3.0. into Albanian, Macedonian, Serbian and Turkish, iPROCEEDS-2
- April-May, C-PROC, (*online*), Translation into French, Spanish and Portuguese of the "Training skill certification Programme for judges and prosecutors delivering Council of Europe judicial trainings on cybercrime and electronic evidence", OCTOPUS
- April-June, C-PROC, (*online*), Further development of the online training platform on cybercrime and electronic evidence, OCTOPUS
- April-July, C-PROC, *(online),* Translation of the HELP Course on Cybercrime and Electronic Evidence into Spanish, Portuguese and French, 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