Cybercrime Digest

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

16 – 31 May 2021

Source: Council of Europe

Date: 31 May 2021

E-evidence Protocol approved by Cybercrime Convention Committee

"The 24th plenary of the Cybercrime Convention Committee (T-CY), representing the Parties to the Budapest Convention, on 28 May 2021 approved the draft "2nd Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. […] Experts from the currently 66 States that are Parties to the Budapest Convention from Africa, the Americas, Asia-Pacific and Europe participated in its preparation. More than 95 drafting sessions were necessary to resolve complex issues related to territoriality and jurisdiction, and to reconcile the effectiveness of investigations with strong safeguards. […] Formal adoption is expected in November 2021 – on the occasion of the 20th anniversary of the Budapest Convention – and opening for signature in early 2022." READ MORE

Source: Council of Europe

Date: 27 May 2021

GLACY+: Webinar Series to Promote Universality and Implementation of the Budapest Convention on Cybercrime

"The Council of Europe Cybercrime Programme Office through the GLACY+ project and the Octopus Project, in cooperation with PGA's International Peace and Security Program (IPSP), are launching a series of thematic Webinars as part of the Global Parliamentary Cybersecurity Initiative (GPCI) to Promote Universality and Implementation of the Budapest Convention on Cybercrime and its Additional Protocol." READ MORE

Source: Europol

Date: 28 May 2021

Industrial-scale cocaine lab uncovered in Rotterdam in latest Encrochat bust

"The cooperation between the French National Gendarmerie (Gendarmerie Nationale) and the Dutch Police (Politie) in the framework of the investigation into Encrochat has led to the discovery of an industrial-scale cocaine laboratory in the city of Rotterdam in the Netherlands. […] In the framework of intelligence activities underway with its operational counterparts, Europol developed actionable intelligence concerning the activities in Europe of this criminal syndicate. In November 2020, Europol brought together the national investigators on both sides who have since been working closely together to establish a joint strategy to bring down the whole network." READ MORE

Source: Politico

Date: 30 May 2021

One group that's embraced AI: Criminals

"[…] Europol, together with cybersecurity firm Trend Micro and the U.N.'s research institute UNICRI, found software that guesses passwords based on an AI-powered analysis of 1.4 billion leaked passwords, allowing hackers to gain access to systems quicker. "The tools become better in quality every time. There's also more tools available to detect and analyze [malicious use of AI], but the question is whether the average business already has access to [these tools]" as they gear up to fight the new threat, said Marietje Schaake, policy director at the Cyber Policy Center at Stanford University and a former member of the European Parliament." READ MORE

Source: Politico

Date: 19 May 2021

Brussels warns Facebook over children's safety on WhatsApp, Messenger

"In an interview with POLITICO on Tuesday, Home Affairs Commissioner Ylva Johansson said she spoke with Facebook's chief lobbyist Nick Clegg, warning him that when the company starts encrypting Messenger, it should leave the door open for photo detection technology that can suss out child pornography.[…] The Commission put forward a temporary proposal in September to allow tech companies to detect and report explicit content and grooming — how sex offenders build relationships with children to exploit them — in private messages and still be compliant with EU privacy laws. […] Now Johansson is thinking about the long term. She wants tech companies to face mandatory detecting and reporting obligations, as well as transparency requirements." READ MORE

Source: Child Hub

Date: 21 May 2021

Campaign launches as new report finds girls at worsening risk of grooming from sexual predators online

"Internet Watch Foundation's (IWF) annual report shows that 11-13-year-old girls are increasingly at risk of grooming and coercion at the hands of online predators. A new campaign is warning teenage girls and their parents about the dangers of being groomed online by sexual predators, who bully and coerce their victims into filming their own sexual abuse on internet-enabled devices, often in the child's own bedrooms in their family homes. The images and videos of this abuse are then shared widely online." READ MORE

Source: Council of Europe

Date: 26 May 2021

iPROCEEDS-2: Online advisory workshop on drafting cybersecurity strategy in Montenegro

"[…] On 24 May, the iPROCEEDS-2 project organised an online workshop on Drafting Policies and Strategies on Cybersecurity, with the aim to provide advices and guidance on drafting a new Cybersecurity Strategy that would be in line with the EU standards. The project will produce an assessment report analysing the current Cybersecurity Strategy against the EU standards on cybersecurity, while indicating the provisions to be included under the new Strategy […]." READ MORE

Source: Inside Privacy

Date: 20 May 2021

Ireland: Major Cyber-attack on Irish Health System Causes Commercial Concern

"On May 20, 2021, there was a major ransomware attack on the Irish health system. The centralized HSE (Health Service Executive), which provides and manages healthcare for the Irish population, was targeted on May 14 and has seen significant disruption since. It has described the attack as a 'zero-day threat with a brand new variant of the Conti ransomware." READ MORE

RELATED ARTICLE:

ZDNet, Ransomware: 'We won't pay ransom,' says Ireland after attack on health service, 17 May 2021

Source: Lexology

Date: 27 May 2021

Ireland: Government publishes Summer Legislation Programme

"Cybercrime Bill – This Bill will give effect to those provisions of the Council of Europe Convention on Cybercrime 2001 not already provided for in national law, in order to enable ratification of the Convention. […] Communications (Data, Retention and Disclosure) Bill – This Bill will revise and replace the Communications (Retention of Data) Act 2011. The Heads of Bill were published in October 2017, following publication of Mr Justice Murray's Report reviewing the 'Law on the Retention of and Access to Communications Data', which found that many features of the 2011 Act are precluded by EU law." READ MORE

Source: The Guardian

Date: 25 May 2021

GCHQ's mass data interception violated right to privacy, court rules

"The UK spy agency GCHQ's methods for bulk interception of online communications violated the right to privacy and the regime for collection of data was unlawful, the grand chamber of the European court of human rights has ruled. […] In Tuesday's ruling, which confirmed elements of a lower court's 2018 judgment, the judges said they had identified three "fundamental deficiencies" in the regime. They were that bulk interception had been authorised by the secretary of state, and not by a body independent of the executive; that categories of search terms defining the kinds of communications that would become liable for examination had not been included in the application for a warrant; and that search terms linked to an individual (that is to say specific identifiers such as an email address) had not been subject to prior internal authorisation." READ MORE

Source: Afrique Media

Date: 26 May 2021

Où en est l'Afrique dans la protection des données personnelles

"A l'heure d'écrire ces lignes, seuls 33 Etats africains ont adopté une loi dédiée à la protection des données et 18 ont mis en place une autorité pour contrôler son application. Et, une fois n'est pas coutume lorsqu'il s'agit de numérique en Afrique, les pays francophones sont les mieux lotis. « Cela s'explique par la mise en place d'une association, l'Association francophone des autorités de protection des données personnelles (AFAPDP), créée en 2007 et qui, très tôt, s'est attelée à sensibiliser les pays francophones sur la question », rappelait Mouhamadou Lô […]." READ MORE

Source: Ministerio Público

Date: 18 May 2021

Panama: "El ciberdelito es real" Ministerio Público y policía nacional lanzan campaña de prevención del delito

"El Ministerio Público y la Policía Nacional realizaron este martes 18 de mayo el lanzamiento de la campaña "El Ciberdelito es Real", dirigida a crear conciencia en la ciudadanía sobre la incidencia, cada vez más alta, de delitos cometidos a través de medios tecnológicos donde personas están siendo víctimas de estafa, extorsión, hurto, robos, delitos contra la seguridad informática, entre otros. […] De acuerdo a estadísticas del Ministerio Público en los últimos cinco años se ha registrado un incremento del 198% en el delito de extorsión, cerrando 2016 con 123 casos, mientras que el 2020 con 424, y en lo que va de 2021 ya se han iniciado 143 investigaciones." READ MORE

Source: CanalTech

Date: 28 May 2021

Brazil: Lei aumenta punições para fraudes e golpes digitais no Brasil; veja o que muda

"Acompanhando o crescimento da ocorrência de golpes digitais e do possível estrago causado por eles, o Governo Federal publicou nesta sexta-feira (28) a Lei 14.155, que prevê punições mais severas para crimes cometidos em meios eletrônicos. O texto modifica o Código Penal e aumenta a condenação para até oito anos de prisão, mais multa, para quem invade dispositivos e/ou realiza furtos qualificados e estelionato usando meios eletrônicos." READ MORE

RELATED ARTICLES:

Portal FEBRABAN, Lei endurece penas para crimes eletrônicos, como clonagem do WhatsApp e outros golpes via internet, 28 May 2021

Minuto da Segurança, Nova Lei nº 14.155 endurece combate ao crime cibernético, 31 May 2021

Source: Enisa

Date: 26 May 2021

Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission

In July 2019, the EUCC was the first candidate cybersecurity certification Scheme request received by the EU Agency for Cybersecurity (ENISA) under the Cybersecurity Act. […] ENISA has developed it with the support of an Ad Hoc Working Group composed of outstanding cybersecurity certification experts, and members of the European Cybersecurity Certification Group (ECCG), that is composed of representatives of the EU Member States." READ MORE

Source: EUROPOL

Date: 28 May 2021

1st referral action day against right-wing terrorist online propaganda

"On 27 May 2021, the 1st Referral Action Day against right-wing terrorist online propaganda was coordinated by the European Union Internet Referral Unit at Europol's headquarters in The Hague. The Action Day was joined by a total of 28 international partners: Australia, Austria, Belgium, Croatia, Czech Republic, Denmark, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Moldova, Montenegro, North Macedonia, Norway, Portugal, Romania, Serbia, Slovakia, Spain, Sweden, United Kingdom, and the New York City Police Department." READ MORE

Source: Bleeping Computer

Date: 27 May 2021

Japanese government agencies suffer data breaches after Fujitsu hack

"Yesterday, the Ministry of Land, Infrastructure, Transport and Tourism and the National Cyber Security Center (NISC) of Japan announced that attackers were able to obtain inside information via Fujitsu's information-sharing tool. Fujitsu also said that attackers had gained unauthorized access to projects that used ProjectWEB and stolen proprietary data. […] By gaining unauthorized access to government systems via ProjectWEB, attackers were able to obtain at least 76,000 e-mail addresses, and proprietary information, including the e-mail system settings, as confirmed by the Ministry of Land, Infrastructure, Transport, and Tourism." READ MORE

Source: Manila Times

Date: 27 May 2021

Philippines: Senate OKs on 3rd reading bill expanding govt protection for children vs online sexual abuse

"Voting 23-0, the Senate on Thursday approved on third and final reading a bill that expands government protection for children against online sexual abuse and exploitation. The senators unanimously passed Senate Bill (SB) 2209 or the proposed Special Protections Against Online Sexual Abuse and Exploitation of Children (OSAEC) Law, or the Anti-OSAEC Law. […] SB 2209 expands the coverage of the Anti-Child Pornography Act of 2009 (RA 9775) and plugs gaps in the law by defining and penalizing OSAEC as a separate crime from those punished under current laws like the Special Protection of Children against Abuse, Exploitation and Discrimination Law (RA 7610) and the Anti-Trafficking in Persons Act (RA 9208)." READ MORE

RELATED ARTICLE:

UNICEF, SaferKidsPH statement on the approval of Senate Bill No. 2209 on the protection of children against online sexual abuse and exploitation, 25 May 2021

Source: INTERPOL

Date: 27 May 2021

Asia: USD 83 million intercepted in INTERPOL operation against online financial crime

"Amid an exponential increase in online fraud, an INTERPOL-coordinated operation codenamed HAECHI-I mobilized more than 40 specialized law enforcement officers across the Asia Pacific region. Over six months of coordinated intelligence collection and joint operations, police were able to intercept a total of USD 83 million in illicit funds transferred from victims to the perpetrators of cyber-enabled financial crime." READ MORE

Latest reports

- UNODC, Cybercrime and covid19 in Southeast Asia: an evolving picture, 16 May 2021
- Enisa, Public Consultation on the draft Candidate EUCC Scheme, 26 May 2021
- National Crime Agency, 2021 National Strategic Assessment (NSA) of Serious and Organised Crime, 25 May 2021
- Institute for Security and Technology, Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force, 2021
- Checkpoint Research, Check Point Research: Asia Pacific experiencing a 168% year on year increase in cyberattacks, May 2021
- MDPI, The Impact of the Development of Society on Economic and Financial Crime. Case Study for European Union Member States, 18 May 2021
- European Court of Human Rights Judgment, BIG BROTHER WATCH and others against the United Kingdom, 25 May 2021
- European Court of Human Rights Judgment, CASE OF CENTRUM FÖR RÄTTVISA v. SWEDEN, 25 May 2021
- Holland Fintech, LexisNexis Risk Solutions: EMEA Cybercrime Report, 26 May 2021
- Politico, The age of surveillance, 26 May 2021
- Seeking Alpha, Why Cloudflare Is Not A Buy Right Now, 31 May 2021
- AI for Tomorrow, L'IA, une révolution dans le domaine de la cybersécurité — Partie 1 — Thierry Berthier, 19 May 2021
- Forensic Science International Digital Investigation, A Hierarchy of Expert Performance (HEP) applied to Digital Forensics: Reliability and Biasability in Digital Forensics Decision Making, May 2021

Upcoming events

- 3 June, C-PROC/BELIZE, (on-line), Stakeholder webinar on new cybercrime legislation, GLACY+
- 3 June, C-PROC, (on-line), 3rd meeting of the Project Steering Committee, iPROCEEDS-2
- 3 June, C-PROC/LEBANON, (on-line), National Workshop for judges, prosecutors and law enforcement on the application of data protection requirements, CyberSouth
- 3-4 June, C-PROC/EAP, (on-line), Joint workshop with EndOCSEA project on Law Enforcement training against child online sexual abuse, CyberEast, EndOCSEA@Europe
- 4 June, C-PROC/LEBANON, (on-line), 3rd Working Group Meeting on the Mainstreaming of Judicial Training Material on Cybercrime and Electronic Evidence
- 10 June, C-PROC, (on-line), 3rd meeting of the Project Steering Committee, CyberEast
- 7 June, C-PROC/MOROCCO, (on-line), National Workshop for judges, prosecutors and law enforcement on the application of data protection requirements, CyberSouth
- 9 June, C-PROC/JORDAN, (on-line), National Workshop for judges, prosecutors and law enforcement on the application of data protection requirements, CyberSouth
- 8-9 June, C-PROC/AZERBAIJAN (on-line), Development of SOPs for CSIRT/LEA, stage II, CyberEast & CybersecurityEast

- 8-9 June, C-PROC/PAPUA NEW GUINEA, (on-line), Introductory Judicial Training on Cybercrime and Electronic Evidence, GLACY+
- 10-11 June, C-PROC/PAPUA NEW GUINEA, (on-line), Workshop on Cybercrime Legislation and Criminal Justice Capacities, GLACY+
- 11 June, C-PROC (on-line), Second webinar to address issues and challenges for chapters 1-5 of the Python Programming for Investigators Online Course, iPROCEEDS-2, GLACY+, CyberEast, CyberSouth, Octopus
- 14-17 June, C-PROC/NETHERLANDS, (on-line), ICANN 71 meeting, GLACY+
- 14-15 June, C-PROC/BARBADOS, Desk review and Online Workshop on Cybercrime Legislation and Electronic Evidence, Octopus project in cooperation with CARICOM IMPACS
- 15 June, C-PROC/ALGERIA, (on-line), National Workshop for judges, prosecutors and law enforcement on the application of data protection requirements, CyberSouth
- By 15 June, C-PROC (desktop study), Preparation of the country profile on OCSEA for Argentina, Octopus , EndOCSEA@Europe
- By 15 June, C-PROC (desktop study), Launch of the survey on the COVID-19 related cybercrime in Asia, Octopus
- By 15 June, C-PROC, Setting up of the proof of concept version of the online training platform, Octopus
- By 15 June, C-PROC, Translation of the Introductory course on cybercrime and electronic evidence into Spanish and Portuguese, Octopus

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 June 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