Cybercrime Digest

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

1-15 November 2020

Source: Council of Europe

Date: 9 Nov 2020

Towards a Protocol to the Convention on Cybercrime: additional stakeholder consultations

"The Cybercrime Convention Committee invites interested stakeholders to submit written comments on draft provisions of the 2nd Additional Protocol to the Budapest Convention by **15 December 2020.** The following new draft provisions have not been subject to previous stakeholder consultations:

- Joint investigation teams and joint investigations
- Expedited disclosure of stored computer data in an emergency
- Request for domain name registration information

The preparation of the 2nd Additional Protocol commenced in September 2017 to address criminal justice challenges in cyberspace and provide for more effective cooperation on cybercrime and electronic evidence. As is the case with the Budapest Convention, the measures in the Protocol are designed for specific criminal investigations only. These measures are subject to strong rule of law and data protection safeguards. The provisions of this Protocol will be of operational and policy benefit and will ensure that the Budapest Convention continues to stand for a free Internet where governments meet their obligation to protect individuals and their rights in cyberspace. Further consultations are envisaged once a complete draft Protocol is available, that is, tentatively in February/March 2021." READ MORE

Source: Council of Europe

Date: 12 Nov 2020

Annual C-PROC activity report published, covering the period October 2019 – September 2020

"The Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania, is responsible for ensuring the implementation of capacity-building projects in the area of cybercrime and electronic evidence, on the basis of the Budapest Convention and in all regions of the world. The present report is to inform the Committee of Ministers of the activities of the Office, from October 2019 to September 2020. C-PROC supported approximately 240 activities over the reporting period. Through the Office, the Council of Europe remains a global leader for capacity building in cybercrime and electronic evidence." READ MORE

Source: Europol

Date: 12 Nov 2020

Europol: How COVID-19-Related Crime Infected Europe During 2020

"The (online and offline) distribution of counterfeit and substandard personal protective equipment, pharmaceutical and sanitary products, including fake 'corona home test kits' and alleged vaccines preventing COVID-19 infection, remains a consistent pandemic-related criminal activity. The area of child sexual abuse material (CSAM) has remained a grave concern during the pandemic; with children spending more time online, the potential increase in demand for CSAM and attempt to engage in child sexual exploitation continues to be a considerable threat. […] Pandemic-themed campaigns have appeared across a wide range of cybercrime activities, including phishing campaigns, ransomware, malware and business email compromise attacks." READ MORE

Source: Council of Europe

Date: 9 Nov 2020

Council of Europe and the International Association of Prosecutors, Webinar on the Second Additional Protocol to the Budapest Convention

"The webinar on "Effective Access to Electronic Evidence: towards a new Protocol to the Budapest Convention", held on November 9th, 2020, was a joint initiative of the Cybercrime Programme Office (C-PROC) of the Council of Europe and the International Association of Prosecutors. During the 2 hours webinar, the panelists discussed about the challenges of international cooperation for access to electronic evidence and the risks to rule of law associated with these. The current proposals on solutions aimed at more effective and efficient access to electronic evidence, including the future 2nd Additional Protocol to the Budapest Convention have also been discussed." READ MORE

Source: Council of Europe

Date: 10 Nov 2020

Pacific Islands Law Officers' Network (PILON), The effects of COVID-19 on cybercrime in the Pacific

"PILON (The Pacific Islands Law Officers' Network) and the Council of Europe teamed up on November 10th in delivering a webinar dedicated to debating the effects of the pandemic on cybercrime in the Pacific. The event gathered more than 50 cybercrime policy makers, criminal justice and law enforcement professionals. In the webinar, panelists discussed the challenges brought by COVID – 19 to cybercrime and stressed the need for effective national cybercrime frameworks aligned to international standards. The recorded session is available here." READ MORE

Source: Threat Post

Date: 13 Nov 2020

Nation-State Attackers Actively Target COVID-19 Vaccine-Makers

"Three major APTs are involved in ongoing compromises at pharma and clinical organizations involved in COVID-19 research, Microsoft says. Three nation-state cyberattack groups are actively attempting to hack companies involved in COVID-19 vaccine and treatment research, researchers said. Russia's APT28 Fancy Bear, the Lazarus Group from North Korea and another North Korea-linked group dubbed Cerium are believed to be behind the ongoing assaults. […] The majority of the targets are vaccine-makers that have advanced to various stages of clinical trials, Burt said – but one is a clinical research organization involved in trials, and one developed a COVID-19 test." READ MORE

Source: Ñuble Actual

Date: 11 Nov 2020

Chile: Avanza votación de mensaje que establece normas sobre delitos informáticos

"La Comisión de Seguridad Ciudadana continuó con la votación particular del proyecto de ley -iniciado en mensaje- que establece normas sobre delitos informáticos, deroga la ley 19.223 y modifica otros cuerpos legales, con objeto de adecuarlos al Convenio de Budapest (boletín 12.192). La iniciativa tiene por objetivo incluir nuevas formas delictivas surgidas a partir del desarrollo de la informática, con el fin de llenar los vacíos del ordenamiento penal en la persecución de ciertas conductas. Ello, a través de la reformulación de los tipos penales contenidos en la actual ley 19.223, como el sabotaje y espionaje informático, adecuándolos a los principios del Convenio de Budapest. READ MORE

Source: The Register

Date: 13 Nov 2020

EncroChat hack evidence wasn't obtained illegally, High Court of England and Wales rules – trial judges will decide whether to admit it

"The contents of messages from encrypted chat service EncroChat may be admissible as evidence in English criminal trials, the High Court in London, England has ruled. A legal challenge to a warrant used by the National Crime Agency for gaining access to hacked data obtained by the French and Dutch authorities has failed, leaving it up to individual judges whether they allow the contents of hacked messages to be used in court or not. The ruling, issued late last month, has profound implications for a number of criminal trials brought over evidence obtained from EncroChat messages. Prosecutors claim that EncroChat was used solely as a means for organised crime gangs to message each other securely and have used the contents of the messages to charge people with crimes involving drugs and gun-running among other things." READ MORE

Source: ZD Net

Date: 6 Nov 2020

Brazilian Superior Electoral Court hit by major cyberattack

"The Brazilian Superior Court of Justice (STJ, in the Portuguese acronym) has been hit by a major cyberattack that will bring its operations to a standstill for an entire week. The incident was detected on Tuesday (3) while several trial sessions were taking place. According to the STJ, a virus was found in the Court's network and, as a precautionary measure, the links to the Internet were disconnected, prompting the cancellation of trial sessions. All the Court's systems, including email, as well as the telephony set up, also became unavailable as a result. STJ minister Humberto Martins released a statement yesterday (5) on the incident, stating that the attack did not affect the information related to the ongoing Court proceedings. According to the minister's note, the invasion blocked access to data using encryption, but there were backups in place." READ MORE

Source: Eurojust

Date: 10 Nov 2020

Coordinated action against illegal online streaming in Switzerland

At the request of the Swiss authorities, Eurojust has coordinated an action day against large-scale piracy and copyright infringements via the illegal streaming of television series and films, operating in Switzerland. In total, 11 servers have been taken down in France, Germany, Monaco, The Netherlands and Switzerland, all offering illegal access to films and TV series without the consent of the rights-holders and depriving the legitimate businesses of over EUR 1.9 million. In the operation, three suspects were arrested by the Swiss authorities, the website promoting the illegal service blocked and eight bank accounts in Switzerland seized. READ MORE

RELATED ARTICLES

Europol, Widely used illegal streaming platform switched off from Switzerland, 11 Nov 2020

Eurojust, Eurojust coordinates action in Italy and ten other countries, taking down over 5.550 computer servers, 11 Nov 2020

Source: Council of Europe

Date: 13 Nov 2020

National Workshop on the cybercrime and e-evidence situation report in Lebanon

"The national meeting to support the preparation of the annual situation report in Lebanon took place on-line on the 12th of November 2020, aiming to discuss the progress made since the regional workshop held in Rabat, in April 2019. This workshop was also an opportunity for the Lebanese institutions to express their views on the cybercrime situation in the country by emphasizing the legal and technical tools for conducting cybercrime investigations and collection of e-evidence as well as the developments on the policies and strategies to fight against cybercrime. The role of a national action plan on combating cyberthreats and annual situation report was underlined and recommendations were given in respect to their structure and actors to be involved. The collection and use of statistics in cybercrime and e-evidence was discussed in depth, with a focus on the methodology for collecting data, structure and its benefits." READ MORE

Source: The Nation

Date: 5 Nov 2020

ECOWAS calls for effective legislation in war against cybercrime

The Economic Community of West African States (ECOWAS) has called for effective legislation in the fight against cybercrime in the sub-region. The call was made at the ongoing ECOWAS Interparliamentary Forum on ICT sessions under the theme: "Role of the Parliamentarian in the fight against cybercrime in the ECOWAS space", from 5 – 7 November 2020 in Niamey, Niger Republic. The ECOWAS Interparliamentary forum on ICT said it recognized that cybercrime in its various forms, especially those that are technology-assisted poses a serious threat to the economies, industry, commerce, banking, and financial services sectors and their operations within the ECOWAS region. The forum noted that cybercrime has become a serious economic threat to negatively impact national and subregional economic development, intra-regional, and external/international trade. READ MORE

Source: Modern Ghana

Date: 9 Nov 2020

Ghana: Parliament has passed the Cybersecurity Act

The Law establishes the Cyber Security Authority, protects the critical information infrastructure of the country, regulates cybersecurity activities, provides for the protection of children on the internet and develops Ghana's cybersecurity ecosystem. It is also targeted at positioning Ghana to prevent, manage and respond to cybersecurity incidents in view of our digital transformation agenda. The memorandum signed by the Minister for Communications, Mrs. Ursula Owusu-Ekuful, indicated that, 'a successful economy is hinged on a secured, safe and resilient national digital ecosystem. Cybersecurity is, therefore, very critical to the economic development of the country and essential to the protection of the rights of individuals within the national digital ecosystem'. READ MORE

Source: RNZ

Date: 5 Nov 2020

Vanuatu: Raft of bills on the table as Vanuatu parliament reconvenes

Fourteen bills are listed for consideration, including the Bill for the Cybercrime Act. The bill enables legal action against new threats such as cyberbullying, stalking and digital hate crimes, while providing important protections for free speech and identity protection. READ MORE

Source: Raaje.mv

Date: 5 Nov 2020

Maldives: Enhancing response capacity of law enforcement agencies is pivotal to protect human rights: minister

Strengthening institutional governance and the response capacity of law enforcement agencies is pivotal to protect human rights, says Minister of Home Affairs, Sheikh Imran Abdulla. The minister made this remark in his address to the Review of Maldives session in the third cycle of the Universal Periodic Review, virtually on Wednesday evening. He presented an intervention on reforming law enforcement agencies and freedom of expression and association at the 26th session of the UPR Working Group. READ MORE

Source: L'Economiste

Date: 4 Nov 2020

Maroc Cybersécurité: Enjeux et réalisations de la stratégie nationale

La pandémie de Covid-19 a favorisé le télétravail, et par la même occasion les cyberattaques ont connu une très forte hausse (voir les chiffres ci-joint, et en particulier l'augmentation de 600% des attaques depuis le confinement comparativement à la même période de 2019). Le Maroc a toujours été précurseur en matière de Cybersécurité depuis 2007, et pourtant le dernier indice mondial de la cybersécurité publié en 2018, par l'Union Internationale des Télécommunications (UIT), le place à la 93e position parmi 174 pays. READ MORE

Source: Krebs on Security

Date: 10 Nov 2020

Ransomware Group Turns to Facebook Ads

"It's bad enough that many ransomware gangs now have blogs where they publish data stolen from companies that refuse to make an extortion payment. Now, one crime group has started using hacked Facebook accounts to run ads publicly pressuring their ransomware victims into paying up. On the evening of Monday, Nov. 9, an ad campaign apparently taken out by the Ragnar Locker Team began appearing on Facebook. The ad was designed to turn the screws to the Italian beverage vendor Campari Group, which acknowledged on Nov. 3 that its computer systems had been sidelined by a malware attack." READ MORE

Source: Europol

Date: 05 Nov 2020

Stopping hate speech online: Europol coordinates first Europe-wide action day

"In the first of its kind, Europol's European Counter Terrorism Centre coordinated a Europe-wide joint action day to target racist and xenophobic hate speech on the internet. The operation, led by Germany, took place in Czechia, France, Germany, Greece, Italy, Ireland, Norway, Spain and the United Kingdom. On the action day, 3 November 2020, law enforcement authorities raided 97 locations and interrogated a number of individuals in relation to offences such as dissemination of racist and xenophobic hate speech, calls to violence and incitement to commit offences. In Germany alone, officers searched 81 houses. The coordinated action targeted communities and individuals spreading hate via the internet using different types of content such as posts, comments, and memes that spread hate and propaganda. The operation, targeting no specific organisations or groups, aimed at preventing hate crime, racism and xenophobia circulating online. […] This first joint action day on hate crimes sends a clear signal to individuals spreading violent hatred on the internet that their actions will be detected." READ MORE

Latest reports

- European Data Protection Supervisor, Opinion on the European Commission proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 Nov 2020
- World Economic Forum, Partnership against Cybercrime, 16 Nov 2020
- ENISA, IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain, 9 Nov 2020
- ENISA, European Rail: Report unveils challenges and stresses the need for investment in cybersecurity, 13 Nov 2020
- Eurojust, Report on Eurojust's casework in the field of the European Investigation Order, 10 Nov 2020
- Circle ID, ICANN Doubles Down on Technical Internet Governance Label: What Are the Implications?, 10 Nov 2020
- Third way, A Roadmap to Strengthen US Cyber Enforcement, 9 Nov 2020
- ICLG, Japan: Cybersecurity Laws and Regulations 2021, 2 November 2020
- UK National Cyber Security Center, Annual Review, Making the UK the Safest Place to live and work online, Nov 2020

Upcoming events

- 17 November, C-PROC, (on-line), Second International Meeting of National Judicial Trainers on Cybercrime and Electronic Evidence, GLACY+, iPROCEEDS-2, CyberSouth
- 17 - 18 November, C-PROC, (on-line), Multi-country TAIEX Workshop on Security Threats amid COVID-19, iPROCEEDS-2
- 17-19 November, C-PROC/Georgia, (on-line), Effective access to data exercise and development of standard procedures between LEA/ISPs, CyberEast
- 18 November, C-PROC, (on-line), Participation in UNICEF experts' consultation to review progress made at national level concerning, EndOCSEA@Europe
- 18 November, C-PROC/Algeria, (on-line), First meeting on the development of domestic Standard Operating Procedures and a toolkit for first responders on cybercrime investigation and e-evidence, CyberSouth
- 18 - 19 November, INTERPOL - 4th Global Conference on Criminal Finances and Cryptocurrencies, iPROCEEDS-2, GLACY+
- 18 - 19 November, C-PROC/Sudan, (on-line), Online advisory workshop on cybercrime and electronic evidence legislation and fundamental rights, GLACY+
- 18-20 November, C-PROC/Cape Verde (on-line), International Conference on Cybercrime for the CPLP countries and online meeting of the Ministers of Justice of the CPLP countries, GLACY+
- 20 November, Online Awareness Campaign launch: New Kiko and the Manymes video and storybook for young children - Campaign addressed to adults, with a focus on parents and caregivers of children 4-7 years old, teaching them how to protect their children and avoid their exposure to phones with video and photo cameras or a webcam, EndOCSEA@Europe
- 23 November, C-PROC, (on-line), First Meeting of the Working Group on Online Training Platform, CyberEast
- 23 November, C-PROC/ Jordan, (on-line), Second meeting on the development of domestic Standard Operating Procedures and a toolkit for first responders on cybercrime investigation and e-evidence, Jordanian Armed Forces, CyberSouth
- 23 November, C-PROC/ Jordan, (on-line), Second meeting on the development of domestic Standard Operating Procedures and a toolkit for first responders on cybercrime investigation and e-evidence - Public Security Directorate, CyberSouth
- 23-27 November, C-PROC, (on-line), INTERPOL Malware Analysis Training - Europe and Africa, GLACY+
- 24 November, C-PROC, (on-line), 2nd Steering Committee Meeting of iPROCEEDS-2, iPROCEEDS-2
- 24-25 November, C-PROC, (on-line), Global Forum on Cyber Expertise Annual V-Meeting 2020, GLACY+
- 24-26 November, C-PROC/Mozambique, (on-line), Advisory on cybercrime legislation and Introductory Training on Cybercrime and electronic evidence for prosecutors, GLACY+
- 25 November, C-PROC/Moldova, (on-line), Support to CyberWeek Moldova (together with CyberSecurity EAST project), CyberEast
- 25 November, C-PROC, (on-line), Law Enforcement training strategies and access to ECTEG training materials, GLACY+, iPROCEEDS-2, CyberEast, CyberSouth
- 25-27 November, C-PROC/Costa Rica/ Chile/ Paraguay (on-line), In Country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strength the 24/7 points of contact for cybercrime and electronic evidence, GLACY+

- 26 November, C-PROC, (on-line), Annual meeting of the 24/7 points of contact, iPROCEEDS-2, CyberSouth, GLACY+, CyberEast
- 26 - 27 November, ITU Forum for Europe on Child Online Protection (presentation) organised within the ITU Regional Initiative for Europe EUR4 on *Enhancing trust and confidence in the use of information and communication technologies*, EndOCSEA@Europe
- 26 November, Bosnia and Herzegovina (Republika Srpska), Domestic meeting to support existing public/private initiatives or establish such mechanisms at domestic level with a focus on cooperation between service providers and criminal justice authorities, Banja Luka, iPROCEEDS-2
- 30 November, (online), Cybercrime Convention Committee (T-CY) 23rd Plenary, GLACY+, iPROCEEDS-2, CyberEast, CyberSouth
- By 30 November, Desk assessment, Albania: Assessment of amendments on the Albanian Penal Code, iPROCEEDS-2
- By 30 November, Botswana, Desk review of Cybercrime and Electronic Evidence Legislation, GLACY+

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