Cybercrime Digest

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

16-31 October 2020

Source: Council of Europe

Date: November 2020

C-PROC preparing new webinars for November

Effective Access to Electronic Evidence: towards a new Protocol to the Budapest Convention**, co-organized with International Association of Prosecutors, **9 November 2020

"The International Association of Prosecutors and the GLACY+ project of the Council of Europe and the European Commission are co-organising a thematic workshop to exchange views and share experiences on the existing and new forms of cooperation for effective access to electronic evidence." READ MORE AND REGISTER HERE

PILON Week Webinar – The effects of COVID-19 on cybercrime in the Pacific**, co-organized with the Pacific Law Officers' Network (PILON), **10 November 2020

"The workshop aims to address the current cybercrime challenges in the COVID19 context in the region and encourage the sharing of experiences and best practices on matters related to cybercrime and e-evidence." READ MORE AND REGISTER HERE

Cyberviolence against Women, 12 November 2020

"[…] in times of ongoing COVID-19 pandemic and continuing restrictions that increase reliance on the Internet, cyberviolence (in general) and cyberviolence against women and girls (in particular) may be even more pervasive than before, calling for more coherent and coordinated approach between governments, the private sector and the civil society." READ MORE AND REGISTER HERE

Source: INTERPOL

Date: 29 Oct 2020

Building a solid foundation for measuring the impact of cybercrime

"INTERPOL and the Council of Europe, in the framework of the GLACY+ Project, […] jointly developed the Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence to support countries develop a clearer vision of the global problem. The key goal of this joint effort is to help criminal justice authorities worldwide acquire the statistics on cybercrime and electronic evidence by providing good practices and recommendations. Statistics enable the authorities to shape effective policies and operational responses. This guide lays out the agenda for compiling criminal justice statistics with key steps for data collection, analysis and cooperation among multiple stakeholders." READ MORE

Source: ENISA

Date: 20 Oct 2020

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected

"Today, the European Union Agency for Cybersecurity (ENISA), with the support of the European Commission, EU Member States and the CTI Stakeholders Group, has published the 8th annual ENISA Threat Landscape (ETL) 2020 report, identifying and evaluating the top cyber threats for the period January 2019-April 2020. This year's publication is divided into 22 different reports, available in pdf form and ebook form. The combined report lists the major change from the 2018 threat landscape as the COVID-19-led transformation of the digital environment." READ MORE

Source: European Council/Council of the European Union

Date: 22 Oct 2020

Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack

"The Council today imposed restrictive measures on two individuals and one body that were responsible for or took part in the cyber-attack on the German Federal Parliament (Deutscher Bundestag) in April and May 2015. This cyber-attack targeted the parliament's information system and affected its ability to operate for several days. A significant amount of data was stolen and the email accounts of several members of parliament, including that of Chancellor Angela Merkel, were affected." READ MORE

Source: Europol

Date: 23 Oct 2020

Jihadist radicalisation: an individual arrested in Spain for spreading terrorist propaganda online

"The Spanish Civil Guard (Guardia Civil) arrested a supporter of the so-called Islamic State terrorist organisation in an operation developed together with Europol. The suspect was searching, editing and further disseminating terrorist propaganda material to young people online. On 20 October, officers from the Spanish authorities arrested a Moroccan citizen in Altea, Alicante suspected of spreading terrorist propaganda online. He was attempting to radicalise and recruit new members for the so-called Islamic State. The suspect was targeting young people via social networks and, to avoid detection from security services, he was later redirecting them to a private messaging application. He was then deepening the radicalisation process while sending them more terrorist propaganda material. Virtually integrated into the so-called Islamic State, the individual shared the violent outlook of the terrorist group and spread it to those he was seeking to recruit online." READ MORE

Source: Le Figaro

Date: 21 Oct 2020

Le gouvernement allemand veut donner aux services secrets l'accès aux conversations chiffrées

"Un projet de loi a été adopté en conseil des ministres et devra encore être validé par les députés du Bundestag. Selon ce texte, l'Office pour la protection de la Constitution, soit les Services de renseignements allemands et le Service de contre-espionnage militaire (MAD) seront à l'avenir autorisés à surveiller non seulement les conversations en cours via Messenger mais aussi les messages cryptés déjà envoyés sur cette plateforme en s'aidant notamment d'un «logiciel espion». «Je ne peux pas accepter que nos autorités de sécurité ne puissent poursuivre les ennemis de notre démocratie par manque de pouvoirs», a expliqué l'initiateur de ce texte, le ministre de l'Intérieur conservateur Horst Seehofer." READ MORE

Source: Cointelegraph

Date: 19 Oct 2020

El cibercrimen se ha disparado en América Latina en plena crisis por el COVID-19

"La región de América Latina se ha convertido en terreno fértil para el ataque de ciberdelicuentes de todo tipo que buscan extorsionar o robar los criptoactivos de sus víctimas. De acuerdo a Kapersky, América Latina registra unos cinco mil ataques de ransomware por día, sin contar las estafas online en Internet que están creciendo en un gran número de países de la región. Lo anterior da cuenta de la escalada en el cibercrimen en latinoamérica, donde los hackers parecen estar encontrado un terreno fértil de vulnerabilidades para hacer de las suyas, en plena crisis por la pandemia del COVID-19 que añade un ingrediente adicional de desespero en las personas para caer en este tipo de ataques." READ MORE

Source: Griffith University

Date: 2 Nov 2020

A New Standard for Pacific Cybercrime Legislation

"In 2016, the government of Vanuatu was rushing to address what was seen by politicians and senior bureaucrats as a rising tide of increasingly intemperate talk, bullying and unwanted information on the internet. This coincided with a global effort by the executive of the International Telecommunications Union, or ITU. Without a mandate from its members, it set out to create a new reference framework for cybercrime law. The campaign reached smaller countries from the Caribbean to sub-Saharan Africa to the Pacific islands. It was a flawed model. A report commissioned by the Council of Europe excoriated the effort. As I reported in the Vanuatu Daily Post in 2016, the model law was 'technically and legally incorrect, confusing, ambiguous', 'poorly drafted', 'unsafe', and of 'dubious' credibility. […] Happily, the bill died on the order table in late 2016. The Public Prosecutor and other stakeholders took advantage of the opportunity to press reset and try again, this time with the assistance of the Council of Europe, which spearheaded the creation of the Budapest Convention, the current international standard for cybercrime. The result is a vastly improved bill. It replaces ambiguity with globally recognised terms and definitions. It makes action against new threats such as cyberbullying, stalking and digital hate crimes easier, but carves out important protections for free speech, the public good, and identity protection." READ MORE

Source: Council of Europe

Date: 27 Oct 2020

Ghana, Cybersecurity Bill tabled for Parliamentary approval, workshop with criminal justice authorities

The Cyber Security Bill is expected "to establish the Cyber Security Authority, to regulate cybersecurity activities in the country, to promote the development of cybersecurity in the country and to provide for related matters". Request for comments was sent to the Council of Europe in June 2020. Further to that request, the Council of Europe provided a preliminary set of comments on the cybercrime aspects entailed by the Bill. A workshop was co-organized by the GLACY+ Project and the Ministry of Communication of Ghana, to finalize discussions on the draft Cyber Security Bill of Ghana and to address specific aspects related to cybercrime, electronic evidence handling and the criminal justice sector. The Bill provides a valuable integration to the current legal framework and will ensure a high level of compliance with the Budapest Convention. The Bill has been tabled in the Parliament in mid-October and it is expected to be adopted by the end of November.

Source: Council of Europe

Date: 30 Oct 2020

Sustainable judicial training on cybercrime in Ghana

"The GLACY+ Project supported the National Cyber Security Center of Ghana in organizing two back-to-back Introductory Judicial Courses on Cybercrime and Electronic Evidence for judges and prosecutors, taking place – respectively – in Kumasi, 19-23 October, covering the northern region, and in Accra, 26-30 October, covering the southern region. The initiative, developed in the context of the National Cyber Security Awareness Month of Ghana, aimed at developing the introductory skills and knowledge required for judges and prosecutors to fulfil their respective roles and functions in cases of cybercrime, electronic evidence and search, seizure and confiscation of online crime proceeds." READ MORE

RELATED ARTICLES

Graphic Online, Increased cybercrimes due to lack of successful investigations and prosecutions, 26 Oct 2020

Source: Kahawa Tungu

Date: 29 Oct 2020

Kenya, High Court nullifies 24 bills including cybercrime law citing lack of involvement by the senate

"The High court has declared a number of bills previously passed by the National Assembly void. This is due to the fact that the assembly failed to involve the senate in the process. The decision arrived at by the three judge bench also affects the law that establishes the Huduma Namba, which was just passed recently, as well as the Computer Cybercrime law." READ MORE

Source: Council of Europe

Date: 28 Oct 2020

Chile focuses on cybercrime and electronic evidence training strategies for judges and prosecutors

"The meeting aimed at assessing the current state of judicial training on cybercrime and electronic evidence and the way forward to ensure the long-term integration of these topics into the training curricula for judges and prosecutors of Chile. Facilitation was provided by two international experts. Specific attention in the design of the judicial training curricula will be put to international cooperation on matters related to cybercrime and relevant aspects of cross-border access to electronic evidence held by multi-national service providers." READ MORE

Source: Council of Europe

Date: 15 Oct 2020

Online domestic workshop on the establishment of the 24/7 point of contact in Albania

"Continuing the series of activities dedicated to the strengthening of the 24/7 Points of Contact established under the Budapest Convention on Cybercrime and to the use of this communication channel, the Joint Project of the European Union and the Council of Europe – iPROCEEDS-2 organized an online domestic workshop and hands-on simulation for improvement of the set-up, competencies and procedures of the Albanian contact point, on 15 October 2020. The workshop gathered representatives of the 24/7 Point of Contact in Albania from the Cybercrime Unit of the Albanian State Police, representatives of the Directorate for Economic and Financial Crimes Department of the Albanian State Police and the Ministry of Justice." READ MORE

Source: DW

Date: 28 Oct 2020

Asamblea Nacional de Nicaragua aprueba Ley especial de ciberdelitos

"La Asamblea Nacional de Nicaragua aprobó este martes la Ley especial de ciberdelitos. Según la bancada oficialista mayoritaria, el objetivo es reordenar y actualizar el marco legal de la materia. De acuerdo a varios diputados opositores y periodistas independientes, violenta los derechos humanos y la libertad de expresión, y limita el ejercicio periodístico. La legislación se aprobó con el voto de 70 diputados de la Alianza Frente Sandinista de Liberación Nacional FSLN contra 16 votos de diputados opositores y la abstención de cuatro legisladores. La nueva ley tiene por objeto prevenir, investigar, perseguir y sancionar los delitos cometidos "por medio de las tecnologías de la información y la comunicación, en perjuicio de personas naturales o jurídicas». El artículo 30 establece que las publicaciones que perjudiquen el honor, el prestigio o reputación de una persona supondrán una pena de entre uno a tres años de prisión." READ MORE

Source: National Assembly of El Salvador

Date: 27 Oct 2020

El Salvador: Crearán mesa técnica para analizar reforma integral a Ley Especial contra Delitos Cibernéticos

"La Comisión de Seguridad Pública y Combate a la Narcoactividad acordó crear una mesa técnica interinstitucional, con el fin de presentar un proyecto de reformas integrales que actualice la Ley Especial contra Delitos Cibernéticos, luego de haber escuchado la ponencia sobre observaciones a dicha normativa de parte del presidente del Comité de Ciberseguridad de la Cámara Americana de Comercio, Héctor Cuchilla. Algunas de las consideraciones presentadas por el presidente del Comité de Ciberseguridad a este marco legal son: la creación de la unidad técnica de investigación de delitos informáticos al interior de la Policía Nacional Civil y Fiscalía General de la República, acreditación de peritos forenses digitales y laboratorios digitales privados, reconocimiento de la figura de identidad digital y los derechos inherentes a esta." READ MORE

Source: Council of Europe

Date: 20 Oct 2020

Training for the Judicial Sector in Turkey on Countering Online Child Sexual Exploitation

"The objective of the training was to enhance the knowledge, skills and capacities of Turkish magistrates to improve their role during OCSEA-related proceedings and mechanisms including with regards to victims and witnesses of such crimes. For this purpose, EndOCSEA consultants presented key international standards and practices to tackle OCSEA in light to the Council of Europe Conventions on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and on Cybercrime (Budapest Convention)." READ MORE

Source: Reuters

Date: 28 Oct 2020

Building wave of ransomware attacks strike U.S. hospitals

"We can still watch vitals and getting imaging done, but all results are being communicated via paper only," the doctor said. Staff could see historic records but not update those files. Experts said the likely group behind the attacks was known as Wizard Spider or UNC 1878. They warned that such attacks can disrupt hospital operations and lead to loss of life. The attacks prompted a teleconference call on Wednesday led by FBI and Homeland Security officials for hospital administrators and cybersecurity experts." READ MORE

Source: krebsonsecurity.com

Date: 28 Oct 2020

Security Blueprints of Many Companies Leaked in Hack of Swedish Firm Gunnebo

"Acting on a tip from Milwaukee, Wis.-based cyber intelligence firm Hold Security, KrebsOnSecurity in March told Gunnebo about a financial transaction between a malicious hacker and a cybercriminal group which specializes in deploying ransomware. That transaction included credentials to a Remote Desktop Protocol (RDP) account apparently set up by a Gunnebo Group employee who wished to access the company's internal network remotely. Five months later, Gunnebo disclosed it had suffered a cyber attack targeting its IT systems that forced the shutdown of internal servers. Nevertheless, the company said its quick reaction prevented the intruders from spreading the ransomware throughout its systems, and that the overall lasting impact from the incident was minimal." READ MORE

Source: Portuguese Government

Date: 20 Oct 2020

Ministra da Justiça destaca papel da PJ no combate à cibercriminalidade

"«Aos reptos a que temos de fazer face, enquanto coletivo nacional, nas dimensões sanitária, social e económica, acrescem os desafios que a prevenção e a repressão da criminalidade económica e financeira, da criminalidade de colarinho branco, da criminalidade organizada, da violência doméstica e da cibercriminalidade colocam às instituições responsáveis pela prevenção e repressão criminal», disse Francisca van Dunem na cerimónia comemorativa dos 75 anos da Polícia Judiciária, onde esteve também o Presidente da República." READ MORE

RELATED ARTICLES

EL PACcTO Project, "A modernização da Justiça é uma área na qual estou pessoalmente empenhada", 28 Oct 2020

Source: The Daily Swig

Date: 28 Oct 2020

Interview: the Anti-Phishing Working Group's Peter Cassidy on finding the antidote to cybercrime

"Sharing threat intelligence could be considered akin to a vaccine in the race to suppress cybercrime campaigns, the Anti-Phishing Working Group's co-founder says. The Anti-Phishing Working Group (APWG) is an international consortium linking businesses, cybersecurity vendors, law enforcement, and government agencies that are all working to clamp down on cybercrime. Security professionals and organizations at large are fighting a constant battle against both existing and emerging threats. Phishing scams are no longer limited to emails claiming the recipient has won the lottery, or messages from phony lawyers representing long-lost relatives worth millions of dollars. Cyber fraudsters now also impersonate well-known and trusted brands with spoofed email addresses, seemingly legitimate but malicious domains, and everything from malvertising to mobile browser overlay techniques are now in play. And as the coronavirus pandemic has contributed its own set of problems, sharing intelligence has become crucial to protecting consumers." READ MORE

Latest reports

- Europol, The Challenges of Countering Human Trafficking in the Digital Era, 18 Oct 2020
- Europol, Operation 2BAGOLDMULE Infographic , 15 Oct 2020
- ENISA, EU Agency for Cybersecurity launches ISAC in a BOX Toolkit, 26 Oct 2020
- FBI, Iranian State-Sponsored Advanced Persistent Threat Actors Threaten Election-Related Systems, 22 Oct 2020
- FBI, Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets, 22 Oct 2020
- CISA/FBI/HHS: Ransomware Activity Targeting the Healthcare and Public Health Sector, October 2020
- Institute for Security Studies Africa, Cybercrime in Nigeria demands public-private action, 19 Oct 2020
- Interisle, Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing, October 2020
- ESET, ESET Threat Report Q3 2020, 28 October 2020
- Dark Reading, Cybercrime Losses Up 50%, Exceeding $1.8B, , 16 Oct 2020
- Abc Net, Work from home revolution during coronavirus pandemic powers spike in cybercrime, 20 Oct 2020
- Blackfog: The State of Ransomware in 2020, October 2020

Upcoming events

- 3 November, C-PROC, (on-line), Second meeting of the CyberSouth Judicial Network, CyberSouth
- 3-4 November, C-PROC/Bosnia and Herzegovina, (on-line), Domestic workshop on drafting policies and strategies in cybercrime and/or cybersecurity areas in line with international standards, iPROCEEDS-2
- 5 November, C-PROC, (on-line), Regional meeting with LEA and presentation of the first responder training course as updated by ECTEG, iPROCEEDS-2
- 5 November, C-PROC, (on-line), African DPA Network Series of Regional Webinars: The right to Data Protection in the Digital Era, GLACY+
- 5 November, C-PROC/Tunisia, (on-line), National Workshop on the preparation of cybercrime and e-evidence situation (annual) report in, CyberSouth
- 9 November, C-PROC/ GLOBAL, (on-line), Webinar on Effective Access to Electronic Evidence: towards a new Protocol to the Budapest Convention, GLACY+
- 10 November, C-PROC/ PACIFIC REGION, (on-line), PILON Regional Workshop on cybercrime and electronic evidence in the Pacific & Pacific Forum on cybercrime and electronic evidence: Policies and Legislation, Capacity Building. On-line session on COVID-19 and Cybercrime, GLACY+
- 11 November, C-PROC/Bosnia and Herzegovina, (on-line), 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, iPROCEEDS-2
- 12 November, C-PROC, (on-line), International webinar on comprehensive sexuality education to prevent self-generated images and/or videos organized in the context of European Day on the Protection of Children Against Sexual Exploitation and Sexual Abuse, EndOCSEA@Europe
- 12 November, C-PROC/Lebanon, (on-line), National Workshop on the preparation of cybercrime and e-evidence situation (annual) report in, CyberSouth
- 12 November, C-PROC, (on-line), Webinar on Istanbul Convention: Cyberviolence against women, CyberEast

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 August 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