Cybercrime Digest

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

1-15 September 2020

Source: EU CYBER DIRECT

Date: 16 Sep 2020

EU Cyber Forum: legal certainty is key for a better international cooperation against cybercrime

"The EU Cyber Forum presented, in its second edition, a range of stimulating conversations about the current shifting situation in cyber-related policy, as determined by the pandemic and the geopolitical landscapes worldwide. Announced as 'a platform for promoting the European Union's global engagement on cyber and digital issues' the Forum addressed the cyberworld in its entirety, as a space where human rights must be respected and responsibility among national, multiregional and multi-level stakeholders has to be equally shared. […] The Budapest Convention stands for a vision of a free Internet, where information can freely flow, be accessed and shared, where restrictions are narrowly defined to counter misuse, and where only specific criminal offences are investigated and prosecuted, subject to the necessary safeguards. The future 2nd Additional Protocol to the Convention will enhance international cooperation through additional tools for direct cooperation with service providers and cooperation in emergency situations." READ MORE

Source: Council of Europe

Date: 16 Sep 2020

Expanding expertise: new series of cybercrime webinars for criminal justice practitioners

A new series of cybercrime webinars has been launched in September by the Cybercrime Programme Office, organized in the context of the GLACY+ Project. The webinars are aiming at addressing specific challenges encountered by criminal justice practitioners in cybercrime investigations and e-evidence related issues. The first three technical sessions, co-organized with INTERPOL and ECTEG as part of the E-FIRST Course for law enforcement, and open to participation of criminal justice authorities worldwide, will focus on: *Crime Scene and Live Data* (21 September), *Mobile Network and Devices* (22 September), *Virtual Asset Seizure* (24 September). A second initiative in this stream will be focusing on collaboration between Law Enforcement agencies and multi-national service providers in cybercrime investigations, co-organized on 30 September 2020 with APWG.EU. Participation of INTERPOL, Facebook, Cloudflare and reps from the criminal justice sector is anticipated. READ MORE

Source: Council of Europe

Date: 3 Sep 2020

Cybersouth: Standard Operating Procedures and toolkit for first responders on cybercrime investigation and e-evidence in Jordan

"Representatives from the Jordanian Armed Forces, the Public Security Department and Computer Forensic Laboratory dealing with cybercrime investigations, e-evidence and handling cybersecurity incidents took part in the event. This activity helped the Jordanian stakeholders to widen their understanding on the benefit of having domestic SOPs in line with international standards, and of showcasing legislative tools and procedures for conducting cybercrime investigations and e-evidence collection." READ MORE

Source: CNBC

Date: 10 Sep 2020

Ireland to reportedly order Facebook to stop sending EU user data to the U.S.

"Ireland's Data Protection Commission has reportedly sent Facebook a preliminary order to stop transferring user data from the EU to the U.S. The DPC could fine Facebook up to 4% of its annual revenue, or $2.8 billion if it failed to comply. It comes just a few months after the European Court of Justice ruled the data transfer standard between the EU and the U.S. doesn't adequately protect European citizen's privacy. […] Facebook declined to comment on the article, but it referred to a blog post published Wednesday." READ MORE

RELATED ARTICLES

Facebook, Securing the Long Term Stability of Cross-Border Data Flows, 9 Sep 2020

Source: INTERPOL

Date: 7 Sep 2020

INTERPOL report highlights impact of COVID-19 on child sexual abuse

"Under-reporting of child sexual abuse and increased sharing of child exploitation material through peer-to-peer networks are among the effects of the COVID-19 pandemic according to an INTERPOL assessment. The report (COVID19 - Child Sexual Exploitation and Abuse threats and trends) highlights the trends and threats in the current context compared to pre-pandemic measures, what impact these are having in the short-term, and what changes are likely to happen as COVID-19 restrictions are changed. […] Key environmental, social and economic factor changes due to COVID-19 which have impacted child sexual exploitation and abuse (CSEA) across the world include: (i) closure of schools and subsequent movement to virtual learning environments; (ii) increased time children spend online for entertainment, social and educational purposes; (iii) restriction of international travel and the repatriation of foreign nationals; (iv) limited access to community support services, child care and educational personnel who often play a key role in detecting and reporting cases of child sexual exploitation. With this increase in obstacles for victims to report offences or access support, there are concerns that some offending may never be reported after a substantial delay." READ MORE

Source: ZD Net

Date: 7 Sep 2020

Chilean bank shuts down all branches following ransomware attack

"BancoEstado, one of Chile's three biggest banks, was forced to shut down all branches on Monday following a ransomware attack that took place over the weekend. "Our branches will not be operational and will remain closed today," the bank said in a statement published on its Twitter account on Monday. Details about the attack have not been made public, but a source close to the investigation said that the bank's internal network was infected with the REvil (Sodinokibi) ransomware. The incident is currently being investigated as having originated from a malicious Office document received and opened by an employee. The malicious Office file is believed to have installed a backdoor on the bank's network, […] used to install the ransomware. […] BancoEstado reported the incident to Chilean police, and on the same day, the Chilean government sent out a nationwide cyber-security alert warning about a ransomware campaign targeting private sector." READ MORE

RELATED ARTICLE

Diario constitucional, A raíz del ciberataque al BancoEstado, 10 Sep 2020

Source: Bleeping Computer

Date: 6 Sep 2020

Netwalker ransomware hits Argentinian government, demands $4 million

"Argentina's official immigration agency, Dirección Nacional de Migraciones, suffered a Netwalker ransomware attack that temporarily halted border crossing into and out of the country. While ransomware attacks against cities and local agencies have become all too common, this may be a first known attack against a federal agency that has interrupted a country's operations. According to a criminal complaint published by Argentina's cybercrime agency, Unidad Fiscal Especializada en Ciberdelincuencia, the government first learned of the ransomware attack after receiving numerous tech support calls from checkpoints at approximately 7 AM on August 27th." READ MORE

Source: Foro Juridico

Date: 14 Sep 2020

El estatus de México y el Convenio sobre la Ciberdelincuencia de Budapest

"México ha mostrado tener un buen modelo de madurez de la capacidad de ciberseguridad, la cual se divide en 5 dimensiones, siendo: (i) política y estrategia de ciberseguridad; (ii) cultura cibernética y sociedad; (iii) educación, capacitación y habilidades en ciberseguridad; (iv) marcos legales y regulatorios; y (v) estándares, organizaciones y tecnologías. Sin embargo, a pesar de que se cuente con altos niveles en su desarrollo cibernético que lo posicione en la región como un exponente en etapas de madurez 2 y 3 (formativa y consolidada) en casi todas las dimensiones, surge la siguiente pregunta: ¿Por qué México no se ha adherido al convenio sobre la ciberdelincuencia, conocido como convenio Budapest? […] Actualmente México se encuentra como observador del Convenio de Budapest y de manera formal ha sido invitado a ascender y adherirse a al mismo. […] El Presidente de la República tendrá que celebrar la adhesión al Convenio de Budapest y esta deberá ser aprobada por el Senado, obligando al país a realizar las reformas pertinentes […]. En una lucha por el derecho, es necesario que la ciudadanía se acerque con sus representantes y externen su interés e importancia de seguir insistiendo para que el Ejecutivo Federal dedique un primer paso a la adhesión, para proseguir con su debida autorización del Senado." READ MORE

Source: Interpol

Date: 2 Sep 2020

Phone scams targeted in INTERPOL-coordinated operation

"Two members of a criminal network engaged in telephone and email fraud have been extradited from China to South Korea, as part of an ongoing operation coordinated by INTERPOL. Operation First Light, first held in 2014, targets telecom fraud and other types of social engineering scams, as well as money laundering of the illicit proceeds. Launched in September 2019, some 37 countries and territories are participating in the latest edition to identify and locate illicit call centres engaged in the fraud scams. […] Another type of social engineering scams encountered during Operation First Light is business email compromise (BEC) fraud, where criminals trick company employees into transferring money into bank accounts they control. In one such case, INTERPOL, Europol and the NCB in Budapest identified money transfers from a Hungarian-based company to three bank accounts in Hong Kong totaling some USD 8.6 million that were made as a result of BEC fraud. With the assistance of the INTERPOL Sub-Bureau in Hong Kong, the transfers were halted and the funds returned the same day." READ MORE

Source: Nikkei Asian Review

Date: 2 Sep 2020

Cambodia plans China-style internet firewall

"The document states the national internet gateway will manage internet connections in the country to enhance national revenue collection, protect national security and assure social order. [...] The gateway will be managed by a government-appointed operator or operators, who will collaborate with the Ministry of Post and Telecommunications, the Telecommunication Regulator of Cambodia and relevant authorities. Among the operator's duties listed in Article 6 of the law is to work with the government to block certain types of content. The operator is "to take actions in blocking and disconnecting all network connections that affect safety, national revenue, social order, dignity, culture, traditions and customs," according to a translation of the law." READ MORE

Source: Reuters

Date: 7 Sep 2020

China to launch initiative to set global data-security rules

"China is launching an initiative to set global standards on data security, countering U.S. efforts to persuade countries to ringfence their networks from Chinese technology, the Wall Street Journal reported on Monday. Under its "Global Initiative on Data Security," China would call on all countries to handle data security in a "comprehensive, objective and evidence-based manner," the Journal said, citing a draft that it had reviewed. The initiative would urge countries to oppose "mass surveillance against other states" and call on tech companies not to install "backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices." Chinese Foreign Minister Wang Yi is scheduled to announce the initiative on Tuesday at a seminar in Beijing on global digital governance, the report said." READ MORE

Source: Cybersecurity and Infrastructure Security Agency

Date: 10 Sep 2020

Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity

"The Cybersecurity and Infrastructure Security Agency (CISA) has consistently observed Chinese Ministry of State Security (MSS)-affiliated cyber threat actors using publicly available information sources and common, well-known tactics, techniques, and procedures (TTPs) to target U.S. Government agencies. CISA has observed these—and other threat actors with varying degrees of skill—routinely using open-source information to plan and execute cyber operations." READ MORE

Source: MIT Technology Review

Date: 10 Sep 2020

North Korean hackers steal billions in cryptocurrency. How do they turn it into real cash?

"In the last decade, Pyongyang has increasingly turned to cybercrime—using armies of hackers to conduct billion-dollar heists against banks and cryptocurrency exchanges, such as an attack in 2018 that netted $250 million in one fell swoop. The United Nations says these actions bring in vast sums which the regime uses to develop nuclear weapons that can guarantee its long-term survival. But there is a big difference between hacking a cryptocurrency exchange and actually getting your hands on all the cash. Doing that requires moving the stolen cryptocurrency, laundering it so no one can trace it, and then exchanging it for dollars, euros, or yuan that can buy the weapons, luxuries, and necessities even bitcoins cannot." READ MORE

Source: PortSwigger

Date: 10 Sep 2020

Changes to Japan's data privacy law echo GDPR

"Japan has made changes to its 2005 Protection of Personal Information (APPI) Act, bringing the bill closer in line with the EU's General Data Protection Regulation (GDPR). The latest tweaks, announced this month, cover data breach reporting and the use of facial recognition data gathered from devices such as security cameras. Breaches should now be reported using an official form, rather than by mail or fax, as before. When processing image data, the intended use should be stated immediately, while the methods and privacy measures used while processing said images should be made clear. These additions follow hard on the heels of more significant changes, which will mean tighter controls on the international transfer of data from 2022, helping to bring the law further in line with GDPR." READ MORE

Source: Business Tech

Date: 2 Sep 2020

South African Parliament to discuss the Cybercrimes Bill in September

"Parliament is set to discuss the Cybercrimes Bill in the coming weeks. Originally introduced in 2017, the Cybercrimes Bill focuses on criminalising the theft and interference of data and bringing South Africa's cybersecurity laws in line with the rest of the world. The objectives of the bill are, among others, to: (i) Create offences and impose penalties which have a bearing on cybercrime; (ii) To criminalise the distribution of data messages which are harmful and to provide for interim protection orders; (iii) To further regulate jurisdiction in cybercrime. "The bill further aims to regulate the powers to investigate cybercrimes, to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes and to provide for the establishment of a 24/7 point of contact," the NCOP (National Council of Provinces) said." READ MORE

Source: Government News

Date: 7 Sep 2020

Australia: Cybercrime reported every 10 mins

"The Australian Cyber Security Centre received one cybercrime report every 10 minutes over the last 12 months, its annual cyber threat report reveals. [...] The nation's critical infrastructure sectors including electricity, water, health, communications and education represented around 35 per cent of the incidents responded to by the ACSC." READ MORE

Latest reports

- Council of Europe, MONEYVAL Committee, COVID-19: Trends in money laundering and terrorism financing, 3 September 2020
- Egmont Group, Combatting child sexual abuse and exploitation
- ASPI, Cybercrime, deterrence and evading attack, 2 September 2020
- ASPI, Covid-19 Disinformation & Social Media Manipulation, 9 September 2020
- ASEAN, Chairman's statement of the 27th ASEAN Regional Forum, 12 Sep 2020
- Malwarebytes, Pandemic caused significant shift in buyer appetite in the dark web, 10 September 2020
- Computer Weekly, Tackling the Post Covid Cybercrime Pandemic, 08 September 2020
- ZD Net, COVID cybercrime: 10 disturbing statistics to keep you awake tonight, 14 September 2020
- Times of India, Virus of Cybercrime: over 3,000 cases every month, 7 September 2020
- The Fiji Times, Cyber crime trends, 12 September 2020
- White House, Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, 4 September 2020
- Weetracker, Kenya Is Africa's Easiest Target for Cyber Attackers, 3 September 2020
- BalkanInsight, Internet Governance Key to Media Freedom in Albania, 10 September 2020

Upcoming events

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.

- 14-18 September (online) - EU Cyber-FORUM, GLACY+, iPROCEEDS-2
- 14-30 September (online) - E-First training Course for GLACY+ countries, in collaboration with ECTEG, INTERPOL, GLACY+
- 16 September (online) - Participation in the ENISA-EC3 Workshop on CSIRT-LEA Cooperation Online event, GLACY+
- 16 September, Lebanon (online) – Meeting on integration of judicial training manual on cybercrime and electronic evidence, CyberSouth
- 21, 22 and 24 September (online) - **Webinars** - 3 technical sessions on E-First training Course for GLACY+ countries, in collaboration with ECTEG, INTERPOL, GLACY+
- 22 September, Morocco (online) – First meeting on the development of national Standard Operating Procedures and a toolkit for First Responders in cybercrime investigations, CyberSouth
- 24 September, Tunisia (online) - First meeting on the development of national Standard Operating Procedures and a toolkit for First Responders in cybercrime investigations, CyberSouth
- 25 September, Georgia (online) - Support to the Georgian Cybersecurity Forum 2020, CyberEast
- 28 – 30 September, Ukraine (online) - Development of Standard Operating Procedures for Cooperation between, CSIRTs and Law Enforcement, CyberEast
- 29 September (online) - Orientation Webinar for the Digital Security Challenge Program, INTERPOL, GLACY+
- 30 September - 2 October, Cape Verde (online) - In Country workshop on data protection and INTERPOL Tools and Services combined with support on how to set-up and strengthen the 24/7 points of contact for cybercrime and electronic evidence, GLACY+
- 30 September (online) - **Webinar** on Collaboration between LEAs and MSP (with participation of INTERPOL, Facebook, Cloudflare and Microsoft), in collaboration with APWG.EU, law enforcement only, GLACY+
- By 30 September, C-PROC - Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation for Albania, iPROCEEDS-2
- By 30 September, C-PROC - Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation for Bosnia and Herzegovina, iPROCEEDS-2
- By 30 September, C-PROC - Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation for Montenegro, iPROCEEDS-2
- By 30 September, C-PROC - Review of the Introductory Judicial Course on Cybercrime and Electronic Evidence, 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