Cybercrime Digest

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

16-30 September 2020

Source: Council of Europe

Date: 24 Sep 2020

New Zealand on course to join the Budapest Convention

New Zealand has been invited by the Council of Europe to accede to the Budapest Convention on Cybercrime. The Government is currently undertaking the necessary domestic measures, including stakeholder consultations, to complete the accession process. New Zealand now also has observer status in the Cybercrime Convention Committee (T-CY), including in the negotiations of the 2nd Additional Protocol to the Budapest Convention that are currently underway. With New Zealand, 65 States are Parties and a further 12 States have signed it or been invited to accede.

Source: Council of Europe

Date: 21 Sep 2020

USA renews support to the global Octopus Project

"The Government of the United States made a new voluntary contribution of USD 1.5 million (approximately €1.3 million) to the Council of Europe's capacity building activities on cybercrime. The US Department of State has supported the project Cybercrime@Octopus since 2014 with approximately €3.5 million to date. This helped increase membership in the Budapest Convention on Cybercrime and strengthen domestic legislation in line with this treaty in all regions of the world. The new contribution will permit the organisation of Octopus Conferences, support the Cybercrime Convention Committee (T-CY) and in particular assist criminal justice authorities worldwide to investigate, prosecute, adjudicate and cooperate on cybercrime more effectively." READ MORE

Source: Council of Europe

Date: 16 Sep 2020

CoE-APWG global webinar focuses on cooperation between criminal justice and service providers

Some 180 representatives from criminal justice authorities of more than 60 countries took part on Wednesday 30 September in the C-PROC global webinar on collaboration between criminal justice authorities and multi-national service providers in cybercrime investigations. The event was co-organized by the GLACY+ Project of the Council of Europe and the APWG.EU, and offered the opportunity to focus on current technical and legal challenges, and highlight current good practices and perspective solutions, also in the light of the innovations that will be introduced by the upcoming Second Additional Protocol to the Budapest Convention.

Source: Council of Europe

Date: 28 Sep 2020

C-PROC: International Call for Consultants

The Cybercrime Programme Office of the Council of Europe (C-PROC) based in Bucharest, Romania has launched an International Call for Tenders aiming to conclude a framework agreement with up to 160 consultants with specific experience of cybercrime and electronic evidence. Please consult the full call below and submit the requested documentation before the deadline on 30 October 2020.

RELATED FILES

Council of Europe, Tender File, 28 Sep 2020

Council of Europe, Act of Engagement, 28 Sep 2020

Source: Council of Europe

Date: 24 Sep 2020

Tunisia, first meeting on SOP and a toolkit for first responders on cybercrime and e-evidence

"Under the framework of the CyberSouth Project, on the 24th of September 2020, an online workshop on Standard Operating Procedures (SOPs) was held for the benefit of Tunisian representatives that deal with cybercrime and e-evidence. The goal was to introduce the benefits, general principles and structure of SOPs on e-evidence as well as to assess whether the existing domestic ones are in line with international standards and best practices. Representatives from the General Directorate for National Security (DGSN), General Directorate of Territorial Surveillance (DGST), National Guard and Computer Forensic Lab took part in the event." READ MORE

Source: Council of Europe

Date: 16 Sep 2020

CyberSouth, Working group to build a manual on cybercrime and electronic evidence in Lebanon

"Under the framework of Cybersouth project, in the period of 3-4 August and 16 of September 2020, the first meeting of the working group in charge of developing a training manual on cybercrime and electronic evidence for Lebanese magistrates was held in the online format. The meeting was aimed at improving the current outline of the module on cybercrime integrated in the initial course for student and in-service magistrates and in the elaboration of the detailed outline of the basic module on cybercrime and electronic evidence." READ MORE

Source: ENISA

Date: 30 Sep 2020

European Cybersecurity Month 2020 'Think Before U Click' kicks off today

"This October marks the European Union's 8th European Cybersecurity Month (ECSM), promoting online security among EU citizens. The annual cybersecurity awareness campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission, and supported by the Member States and more than 300 partners from across industries. Hundreds of activities, such as conferences, workshops, training sessions, general presentations, webinars and online campaigns, will take place across Europe for the entire month of October to raise awareness of cybersecurity and provide up-to-date digital security information through education and sharing of good practices. Each year, the European Cybersecurity Month brings together EU citizens to join forces under the slogan 'Cybersecurity is a Shared Responsibility' to unite against cyber threats." READ MORE

Source: Breaking Belize News

Date: 26 Sep 2020

Belize, Cyber Crime Bill approved by House of Representatives

"The bill had bipartisan support and in response to questions about certain aspects of the legislation, Minister of Education with responsibility for technology, Patrick Faber, made note that the legislation always has an opportunity for amendment even before it is passed into law, starting with the House Committee, in the House itself, at the Senate and afterwards. [...] Faber said there are layers to crimes legislated, so that "illegal access to a computer system is an offence, illegal access to the data off that computer will be an offence, illegal interference of that data will be an offence," and each is charged separately." READ MORE

Source: Europol

Date: 22 Sep 2020

International sting against dark web vendors leads to 179 arrests

"Today, a coalition of law enforcement agencies across the world announced the results of a coordinated operation known as DisrupTor which targeted vendors and buyers of illicit goods on the dark web. This operation follows the takedown in May of last year of Wall Street Market, the world's then second largest illegal online market in the dark web. Led by the German Federal Criminal Police (Bundeskriminalamt) with the support of the Dutch National Police (Politie) Europol, Eurojust and various US government agencies, this takedown provided investigators with quantitative data and materials to identify suspects behind dark web accounts used for illegal activity. As a result, 179 vendors who engaged in tens of thousands of sales of illicit good were arrested across Europe and the United States. Over $6.5 million were seized in both cash and virtual currencies, alongside some 500 kilograms of drugs, including fentanyl, oxycodone, hydrocodone, methamphetamine, heroin, cocaine, ecstasy, MDMA, and medicine containing addictive substances; and 64 firearms." READ MORE

RELATED ARTICLES

FBI, Operation DisrupTor, 22 Sep 2020

Wired, 179 Arrested in Massive Global Dark Web Takedown, 22 Sep 2020

Source: INTERPOL

Date: 17 Sep 2020

Brazilian arrested for production and global distribution of child sexual abuse material

"A referral sent to Brazilian authorities by INTERPOL's Crimes against Children unit has led to the arrest of a suspected child sexual abuser who, for years, posted images and videos of his crimes online. Operation 'Unveiled' was carried out by the Brazilian Federal Police's Child Exploitation Unit (NURCOP) after receiving intelligence from the INTERPOL General Secretariat headquarters in Lyon, France. The information was based on material uploaded to INTERPOL's International Child Sexual Exploitation database in 2017 by Australian officers, which was later complemented by uploads from Denmark and the INTERPOL Victim Identification Task Force. The photos and videos depicted the explicit sexual abuse of two girls aged approximately three and 10 years old. The offender had posted the material in several Darknet forums, which had hundreds of thousands of registered users. One of those forums is believed to be the largest Portuguese-language child sexual abuse forum on the Darknet." READ MORE

Source: Europol

Date: 24 Sep 2020

Hackers Arrested in Poland In Nation-Wide Action Against Cybercrime

"Today, the Polish authorities are announcing the arrest of 4 suspected hackers as part of a coordinated strike against cybercrime. Those arrested are believed to be among the most active cybercriminals in the country. This operation was carried out by the Polish Police Centre Bureau of Investigation (Centralne Biuro Śledecze Policji) under the supervision of the Regional Prosecutor's Office in Warsaw (Prokuratura Regionalna w Warszawie), together with the cybercrime departments of provincial police headquarters and Europol. These 4 suspects are believed to be involved in a wide variety of cybercrimes, including: Malware distribution [...], SIM swapping [...], E-commerce fraud." READ MORE

Source: Eurojust

Date: 29 Sep 2020

Eurojust supports successful takedown in Romania of an OCG carrying out elaborated cybercrime and bank frauds in Lithuania and Estonia

"With active judicial support of Eurojust, the Romanian, Lithuanian and Estonian authorities have executed coordinated activities, within a Joint Action Day, to dismantle an Organised Crime Group (OCG) specialized in elaborate cybercrime and fraudulent financial operations, arresting 3 suspects and conducting 4 house searches. The OCG allegedly committed identity theft and lured bank customers in several countries into imputing their access credentials online, via text messages containing links to cloned bank sites, subsequently the perpetrators accessing the victims' accounts and making fraudulent transfers into specially-created accounts they directly controlled. Eurojust played a pivotal role in the entire operation by setting up and financing a Joint Investigation Team and facilitating the continuous judicial cooperation between the involved National Authorities." READ MORE

Source: FBI

Date: 17 Sep 2020

Iranian malware used to monitor dissidents and travel and telecommunication companies

"Today, the Federal Bureau of Investigation released a new cybersecurity advisory to academic, public, and private sector partners across the country about previously undisclosed malware attributed to Iranian nation state actors publicly known as Advanced Persistent Threat 39 (APT 39), Chafer, Remexi, Cadelspy, or ITG07. [...] Masked behind its front company, Rana Intelligence Computing Company (Rana), the Government of Iran's Ministry of Intelligence and Security (MOIS) has employed a years-long malware campaign that targeted and monitored Iranian citizens, dissidents, and journalists, the government networks of Iran's neighboring countries, and foreign organizations in the travel, academic, and telecommunications sectors. Some of these individuals were subjected to arrest and both physical and psychological intimidation. [...] At least 15 U.S. companies were compromised by Rana's malicious cyber intrusion tools, all of which the FBI has notified, along with hundreds of individuals and entities from more than 30 different countries across Asia, Africa, Europe, and North America." READ MORE

RELATED ARTICLES

U.S. Department of Justice, State-Sponsored Iranian Hackers Indicted for Computer Intrusions at U.S. Satellite Companies, 17 Sep 2020

Source: AllAfrica

Date: 16 Sep 2020

Nigeria: New Report Seeks Repeal, Re-Enactment of Cybercrime Act 2015

"A new report that explores the state of digital rights and privacy in Nigeria that was launched by Paradigm Initiative, a Pan-African Digital Rights and Inclusion organisation, is seeking for the repeal and re-enactment of the Cybercrime Act 2015, among others. The report, which was launched during a recent civil society webinar on Nigeria's draft data protection bill focused on Nigeria's political and policy environment as well as practices around digital rights and privacy. Aside recommending the repealing and re-enactment of the Cybercrimes Act 2015, the report also recommended the passage of the digital rights and freedom bill and the data protection bill, in order to raise public awareness of citizens on data protection." READ MORE

Source: RTB

Date: 18 Sep 2020

Burkina Faso, un réseau de cyber escrocs appréhendé

"La Brigade Centrale de Lutte contre la Cybercriminalité (BCLCC) était face à la presse ce vendredi 18 septembre 2020 pour présenter un réseau de Cyber escrocs spécialisés dans l'arnaque en ligne. Suite à plusieurs plaintes portées par des victimes, la BCLCC a ouvert une enquête ayant abouti à l'interpellation d'un réseau de Cyber escrocs spécialisés dans l'arnaque en ligne. [...] Les membres du réseau promettaient aux victimes d'envoyer leurs articles via les compagnies de transport de la place ; une forme de livraison un peu partout au Burkina Faso. Malheureusement, les victimes ne rentreront jamais en possession de leurs articles après avoir rempli toutes les conditions. [...] En seulement sept mois d'existence, la Brigade Centrale de Lutte Contre la Cybercriminalité qui a pour mission de lutter contre les infractions en matière informatique interpelle les internautes à plus de prudence et à toujours dénoncer tout cas suspect." READ MORE

Source: al Khaleej

Date: 24 Sep 2020

Thailand takes first legal action against Facebook, Twitter over content

"Thailand began legal action today against Facebook and Twitter for ignoring requests to take down content, in its first such move against major internet firms. The digital ministry filed legal complaints with cybercrime police after the two social media companies missed 15-day deadlines to comply fully with court-issued takedown orders from Aug. 27, the digital minister, Puttipong Punnakanta, said. No action was taken against Alphabet's Google as originally suggested, as it took down all the YouTube videos specified in the order late yesterday, Puttipong said. "This is the first time we're using the Computer Crime Act to take action against platforms for not complying with court orders," Puttipong told reporters. "Unless the companies send their representatives to negotiate, police can bring criminal cases against them. But if they do, and acknowledge the wrongdoing, we can settle on fines." READ MORE

Source: Lexology

Date: 25 Sep 2020

Ireland, New Government Legislation Programme Published

"Preparatory work has also begun on the Cybercrime Bill, to introduce the remaining provisions of the Council of Europe Convention on Cybercrime9 into Irish law so that the Convention may be ratified." READ MORE

Source: Engadget

Date: 25 Sep 2020

The next generation of wearables will be a privacy minefield

"Facebook recently gave us our best glimpse yet into its augmented reality plans. The company will be piloting a new set of glasses that will lay the groundwork for an eventual consumer-ready product. The "research project," called Project Aria, is still in very early stages, according to Facebook. There's no display, but the glasses are equipped with an array of sensors and microphones that record video, audio and even its wearer's eye movements — all with the goal of helping scientists at Facebook's Reality Labs "figure out how AR can work in practice." READ MORE

Latest reports

- D. Wicki-Birchler, The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?, International Cyber Security Law Review, Springer, 22 Sep 2020
- U.S. Cybersecurity and Infrastructure Security Agency, Federal Agency Compromised by Malicious Cyber Actor, 24 Sep 2020
- Council of Europe, Publication of the first progress report of the Ad hoc Committee on Artificial Intelligence (CAHAI), 29 September 2020
- Microsoft Digital Defense Report, September 2020
- Centro Criptológico Nacional CERT, Memoria de Actividades 2019, (ES&EN versions report), 23 Sep 2020
- The Fintech Times, New Cybercrime Report Reveals Opportunities and Risks for EMEA Online During Global Pandemic, 22 September 2020

Upcoming events

- Starting with 1 October, Cooperation with regional training centers, GLACY+
- 1 October, Lebanon (online) - First national meeting on the development of domestic Standard Operating Procedures and a toolkit for first responders on cybercrime investigation and e-evidence, CyberSouth
- 2 October, Desk Study, Report on Cybercrime Statistics, in collaboration with INTERPOL, GLACY+
- 5 October, Ukraine (online) - Webinar on Online Child Sexual Exploitation and Abuse for Ukrainian professionals (Law Enforcement, Prosecutors, Judges), EndOCSEA@Europe
- 5-7 October, Georgia (online) - Technical exercise on elections security, CyberEast
- 5-9 October, Asia-Pacific (online) - INTERPOL Malware Analysis Training, GLACY+
- 6 October (online) - INTERPOL-Europol Annual Conference on Cybercrime, GLACY+
- 6 October, Serbia (online) - Domestic workshop and hands-on simulation for improvement of the skills, set-up and competencies of 24/7 points of contact, iPROCEEDS-2
- 7-9 October, Turkey (online) - Specialized training course on Online Child Sexual Exploitation and Abuse and handling of electronic evidence, iPROCEEDS-2, EndOCSEA@Europe
- 8 October, Germany, Hamburg (online) - ICANN 69 GAC PSWG, GLACY+
- 8 October, Tunisia (online) - National workshop on cybercrime procedural law, CyberSouth
- 12-13 October, Georgia (online) - Workshop on crime proceeds and reporting systems, CyberEast
- 12-16 October and 20 October (online, follow-up webinar) INTERPOL Digital Security Challenge Program, GLACY+
- 14 October, Algeria (online) - National workshop on cybercrime procedural law, CyberSouth
- 15 October Albania (online) - Domestic workshop and hands-on simulation for improvement of the skills, set-up and competencies of 24/7 points of contact, iPROCEEDS-2
- By 15 October, Albania, Desk Review - Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- By 15 October, Bosnia and Herzegovina, Desk Review - Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- By 15 October, Montenegro, Desk Review - Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2

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