Cybercrime Digest

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

16 - 30 November 2020

Source: C-PROC

Date: 1-10 Dec 2020

GLACY+ INTERPOL Technical Webinars on Crypto for Criminal Justice Authorities

Between 1 and 10 December, in the framework of the GLACY+ Project, INTERPOL is organising a series of 5 technical webinars to provide basic knowledge and conceptual understanding of cryptography and related topics, including digital certificates and cryptocurrencies, specifically targeting criminal justice authorities, law enforcement officers and instructors of governmental institutions responsible for the training on this topic. Registrations and other details are provided here.

Source: Council of Europe for GFCE

Date: 24 Nov 2020

GFCE, Building capacities on cybercrime in times of COVID-19

"COVID-19 pandemic had a direct impact on the cybercrime global landscape, with malicious actors exploiting vulnerabilities of individuals in a period when criminal justice authorities were facing increasing challenges due to the mutated priorities and the different working conditions. In such a scenario, capacity building was deemed useful as long as it could provide concrete responses and usable solutions to the emerging necessities and the related requests. Programs in the field were able to support by reassessing the needs of the beneficiaries, adapting the work plan and redesigning efficient delivery methods." READ MORE

Source: INTERPOL

Date: 5 Nov 2020

COVID-19 crime: INTERPOL issues new guidelines for law enforcement

"These updated INTERPOL guidelines draw on the lessons learned and best practices developed around the world to help police identify and address crimes impacted by COVID-19, including domestic violence, child abuse and cybercrime. The pandemic has provided an opportunity for criminals to make fast cash as they take advantage of the high demand for personal protective equipment. Operations coordinated by INTERPOL, such as Pangea XIII and Qanoon, targeting the illicit online sale of medicines have shown the continued trend in the dangerous trafficking of medical products related to COVID-19." READ MORE

Source: Council of Europe

Date: 24 Nov 2020

Japan makes a voluntary contribution to support the global Cybercrime@Octopus project

"The Government of Japan has renewed its support to the Council of Europe's work against cybercrime, making a voluntary contribution to the current Cybercrime@Octopus project aimed at assisting countries worldwide to implement the Budapest Convention on Cybercrime and strengthen data protection and rule of law safeguards. Japan has been promoting global implementation of the Budapest Convention for many years, supporting organization of Octopus Conferences on Cooperation against Cybercrime and other important activities, and acting as a strong supporter of the Budapest Convention in international fora such as the Global Conferences on Cyberspace and UN Congress for Crime Prevention and Criminal Justice." READ MORE

Source: tpa.ao

Date: 11 Nov 2020

CPLP: COVID-19: como combater o cibecrime em tempo de pandemia

"No âmbito do Projecto GLACY+ em parceria com o programa da Presidência de Cabo Verde da Conferência dos Ministros da Justiça dos Países de Língua Oficial Portuguesa (CMJPLOP), cujo tema é "Combater o cibercrime: Um novo desafio para a justiça", decorreu de 18 a 20 do corrente mês por via virtual a conferência internacional sobre Cibercrime e Cooperação Internacional durante a Pandemia de Covid-19 na Comunidade dos Países de Língua Oficial Portuguesa. Os países da CPLP reunidos - Angola , Brasil, Cabo Verde, Guiné-Bissau, Guiné Equatorial, Moçambique, Portugal, São Tomé e Príncipe e Timor-Leste - renovaram as recomendações feitas na Conferência de Sal de 2019, pela ocasião da XVI Conferência dos Ministros da Justiça da CPLP e, recomendaram aos Estados Membros que integrem a Convenção de Budapeste, [...] e que se empenhem em dar início a estudos aprofundados das suas legislações nacionais e iniciem os procedimentos necessários à sua ratificação ou adesão. Ainda considerando a dificuldade extrema imposta pela situação actual os Estados Membros recomendam que haja um fortalecimento das unidades especializadas no serviço policial, através da criação/reforço de unidades de investigação de crimes cibernéticos, segundo indicado nas recomendações gerais pelo Sr. Benvindo Oliveira, diretor da Direção Geral da Política de Justiça, do Ministério da Justiça e Trabalho de Cabo Verde." READ MORE

Source: HRD

Date: 1 Dec 2020

Vaccine maker AstraZeneca staff 'targeted' in cyber attack, allege reports

"Hackers have been targeting AstraZeneca employees in a recent cyberattack attempt against the COVID-19 vaccine frontrunner, according to Reuters. The hackers, suspected to be from North Korea, allegedly acted as recruiters and contacted employees on online networking platforms like LinkedIn and WhatsApp with fake job offers, according to media reports. After the bait, they sent job descriptions through documents filled with malicious viruses that would allow access to AstraZeneca's systems. The cyberattack attempt is known to be unsuccessful, reported Reuters. AstraZeneca declined to comment, but University of Oxford, their partner in the vaccine R&D process, told CNN that they're working with the UK National Cyber Security Centre to ramp up cybersecurity efforts and protect their work. CNN also reported that North Korean officials have denied all allegations and labelled the story as 'fake news' and 'fabricated'. US officials and cybersecurity experts suspected North Korean hacking organisations as the attack aligned with similar, ongoing campaigns." READ MORE

Source: Europol

Date: 25 Nov 2020

Virtual tabletop exercise coordinated by Europol: disrupting terrorism and violent extremism online

"On 23 November 2020, the EU Internet Referral Unit (EU IRU) hosted their second tabletop exercise in a virtual event held under the umbrella of the European Commission-led EU Internet Forum. The aim of the exercise was to test an EU-led voluntary mechanism to enable a coordinated response to a cross-border massive abuse of the internet in the context of terrorism or violent extremism. The EU IRU's initial tabletop exercise, held on 11 September 2019, was the first of its kind since the launch of the Christchurch Call to Action and led towards closer cooperation between parties involved in advancing the fight against terrorism online." READ MORE

Source: Solomon Times

Date: 17 Nov 2020

Canada, cybersecurity agency calls out four countries as the 'greatest strategic threats' to Canada

"Canada's top cybersecurity agency has named China, Russia, Iran, and North Korea's state-sponsored cyber activity as posing the "greatest strategic threats" to Canada's critical infrastructure, intellectual property, and political events like elections. In its 2020 National Cyber Threat Assessment, the Canadian Centre for Cyber Security within the Communications Security Establishment warns that state-sponsored cyber activity is the most sophisticated and actors are "very likely" attempting to develop capabilities to disrupt critical systems; will "almost certainly" continue conducting commercial espionage against Canadian governments, businesses, and organizations; and are keeping up ongoing online foreign influence campaigns aimed at altering discourse around current events to divide Canadians." READ MORE

Source: The Cable

Date: 19 Nov 2020

Nigeria, Police launch cybercrime reporting portal for 'prompt' investigation of suspects

"In a statement on Thursday, the police said the portal will enable prompt investigation, arrest and prosecution of perpetrators of cybercrime and other related offences. According to the police, victims or complainants can now report internet-related criminal activities online, at any time and from any part of the world — the portal can be accessed here. "The cases are promptly attended to by the cybercrime unit of the force domiciled with the INTERPOL National Central Bureau (NCB), Force Headquarters, Abuja and the newly created Cybercrime Unit at the INTERPOL Annex, Alagbon Close, Ikoyi, Lagos," the statement read." READ MORE

Source: C-PROC

Date: 18 Nov 2020

Development of domestic SOPs and a toolkit for first responders on cybercrime and e-evidence in Algeria

In the framework of the CyberSouth Project, an online workshop was held on Standard Operating Procedures (SOPs) addressing Algerian law enforcement officers that deal with cybercrime and e-evidence. The activity fostered the use of domestic SOPs in line with international standards and presented legislative tools and procedures for conducting cybercrime investigations and collecting e-evidence from the crime scene. Participants presented their domestic SOPs and assessed their compliance with international standards and best practices. READ MORE

Source: ZD Net

Date: 27 Nov 2020

A hacker is selling access to the email accounts of hundreds of C-level executives

"Access is sold for $100 to $1500 per account, depending on the company size and exec role. A threat actor is currently selling passwords for the email accounts of hundreds of C-level executives at companies across the world. The data is being sold on a closed-access underground forum for Russian-speaking hackers named Exploit.in. […] A source in the cyber-security community who agreed to contact the seller to obtain samples has confirmed the validity of the data and obtained valid credentials for two accounts, the CEO of a US medium-sized software company and the CFO of an EU-based retail store chain." READ MORE

Source: Council of Europe

Date: 18 Nov 2020

Sudan moves towards Cybercrime and E-Evidence Legislation in line with international standards

"The Government of Sudan and the Council of Europe, through the Cybercrime Division and the Data Protection Unit, have kick-started a collaboration […] aimed at having a new cybercrime law in line with the international standards provided by the Budapest Convention. An online workshop […] was organized on November 18 and 19 […] in the framework of the GLACY+ project and in collaboration with the Ministry of Justice of Sudan. […] A comparative analysis between the current legal framework and the Budapest Convention was presented and recommendations on possible amendments discussed." READ MORE

Source: Expresso das Ilhas

Date: 26 Nov 2020

Cape Verde : Rede Tecnológica Privativa do Estado suspensa devido a ciberataque

"Os serviços da Rede Tecnológica Privativa do Estado (RTPE) estão temporariamente suspensos após ataque pelo RANSOMWARE detectado em alguns segmentos da rede, informa o Núcleo Operacional de Sociedade Informação, em comunicado. "Alguns segmentos da Rede Tecnológica Privativa do Estado (RTPE) estão a ser fortemente atacados pelo RANSOMWARE. Por razões de segurança e com vista a evitar a sua propagação em toda rede, os serviços na RTPE serão temporariamente suspensos", explica. Entretanto, as equipas do NOSi estão a tentar repor o normal funcionamento da RTPE, "o quanto antes"." READ MORE

Source: The Star

Date: 23 Nov 2020

Malaysia, outdated laws to be amended to fight cybercrime, says minister

"Amendments will be made to older laws to help deal with growing cybercrime, says Minister in the Prime Minister's Department Datuk Seri Mohd Redzuan Md Yusof. "The government is ready to review and amend existing laws, such as the Computer Crimes Act 1997, which are considered outdated in light of developments in technology," he said when winding up his ministerial replies on Budget 2021 in the Dewan Rakyat on Monday (Nov 23). He said the review of these law was in line with the National Cyber Security Strategic Plan 2020-2024 that was launched last month." READ MORE

Source: O Pais

Date: 24 Nov 2020

Mozambique, Cibercrimes aumentaram de 463 para 798 casos entre 2019 e 2020

"Os cibercrimes aumentaram de 463 casos, de Janeiro a Outubro de 2019, para 798, em igual período deste ano. A informação foi avançada pela Procuradoria-Geral da República, durante um seminário sobre a matéria dirigido a procuradores, juízes e investigadores do Serviço Nacional de Investigação Criminal (SERNIC). Com a pandemia da COVID-19, as plataformas digitais foram o caminho que muitos moçambicanos encontraram para se reinventar e garantir o seu sustento. Mas a implicação foi o aumento em 72% dos crimes, em que se utiliza um computador ou uma rede de computadores como instrumento ou base de ataque, comparativamente ao ano passado." READ MORE

RELATED ARTICLES

Council of Europe, Strengthening cybercrime legislation and criminal justice international cooperation in Mozambique, 26 Nov 2020

Source: INTERPOL

Date: 25 Nov 2020

Three arrested as INTERPOL and the Nigeria Police Force disrupt prolific cybercrime group

"Three suspects have been arrested in Lagos following a joint INTERPOL, Group-IB and Nigeria Police Force cybercrime investigation. The Nigerian nationals are believed to be members of a wider organized crime group responsible for distributing malware, carrying out phishing campaigns and extensive Business Email Compromise scams. The suspects are alleged to have developed phishing links, domains, and mass mailing campaigns in which they impersonated representatives of organizations. They then used these campaigns to disseminate 26 malware programmes, spyware and remote access tools, including AgentTesla, Loki, Azorult, Spartan and the nanocore and Remcos Remote Access Trojans. These programmes were used to infiltrate and monitor the systems of victim organizations and individuals, before launching scams and syphoning funds. According to Group-IB, the prolific gang is believed to have compromised government and private sector companies in more than 150 countries since 2017." READ MORE

Source: Solomon Times

Date: 17 Nov 2020

Solomon Islands Cabinet Passes Ban on Facebook

"Cabinet has agreed to ban the world's biggest social networking site, Facebook, in Solomon Islands. Said to be a temporary measure the submission for the ban on Facebook was said to be brought to Cabinet by the Prime Minister Manasseh Sogavare and Communication and Civil Aviation Minister Peter Shanel Agovaka. Minister Agovaka told Solomon Times Online (STO) that this temporary ban was made because of the controversial issues raised via Facebook. "Abusive languages against Ministers, Prime Minister, character assasination, defamation of character, all these are issues of concerns", Agovaka says. He says there were concerns that there are also no laws or regulations on Facebook thus the need for such a temporary ban." READ MORE

RELATED ARTICLES

Solomon Times, Facebook Ban not a Solution, 17 Nov 2020

Source: Ifex

Date: 27 Nov 2020

Iraq: Vague cybercrime bill threatens free expression

"This statement was originally published on **hrw.org** on 25 November 2020. Iraqi lawmakers are considering a draft law on information technology crimes that could be used to stifle free expression, Human Rights Watch said today. Free speech is already under attack in Iraq, and on November 23, 2020 lawmakers discussed this draft law and planned to hold a second reading during the week of November 29. The bill includes vague provisions that will allow Iraqi authorities to harshly punish expression they decide constitutes a threat to governmental, social, or religious interests. "This law would give Iraqi authorities yet another tool to suppress dissent over the main medium that journalists, activists, and the general public rely on for information and open debate," said Belkis Wille, senior crisis and conflict researcher at Human Rights Watch. "If parliament passes the law, it will further undermine the already narrow field for free speech and stifle public discussion and debate online." READ MORE

Latest reports

- Europol, SIRIUS Project, EU digital evidence situation report - 2nd annual report, 1 Dec 2020
- UN, Joint Statement on Data Protection and Privacy in the COVID-19 Response, 18 Nov 2020
- UNICRI, New Report Finds that Criminals Leverage AI for Malicious Use – And It's Not Just Deep Fakes, 19 Nov 2020
- PILON, Mutual Legal Assistance Handbook: Cybercrime and Electronic Evidence
- ENISA, Cybersecurity Stocktaking in the CAM, 20 Nov 2020
- ENISA, Telecom Security During a Pandemic, 26 Nov 2020
- Harvard Law School Forum on Corporate Governance: Cyber: New Challenges in a COVID-19–Disrupted World, 23 Nov 2020
- ZD Net, 2020's worst cryptocurrency breaches, thefts, and exit scams, 1 December 2020
- Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 13 Nov 2020
- Dark Reading, How Cyberattacks Work, 20 Nov 2020
- ZD Net, The ransomware landscape is more crowded than you think, 16 Nov 2020

Upcoming events

- 1-3 December, T-CY, (on-line) 7th Protocol Drafting Plenary, Cybercrime@Octopus
- 2-4 December, C-PROC/Moldova (on-line), Effective access to data exercise and development of standard procedures between LEA/ISPs, CyberEast
- 3 December, C-PROC, (on-line), Coordination meeting with Joint CoE project from Turkey and EndOCSEA team to set up the training for magistrate judges and prosecutors on OCSEA in Turkey, iPROCEEDS-2
- 3-4 December, C-PROC/Netherlands, (on-line), Contribution to Eurojust SIRIUS Project Meeting, CyberEast
- 4 December, C-PROC, (on-line), 2nd Working Group meeting on the development of the on-line training platform, Cybercrime@Octopus, GLACY+, iPROCEEDS-2, CyberSouth, CyberEast
- 7 December, C-PROC, (on-line), CyberEast Project Steering Committee, CyberEast
- 7-11 December, C-PROC, (on-line), INTERPOL Malware Analysis Training – AMERICAS, GLACY+
- 8 December, C-PROC, (on-line), African Data Protection Authorities Network Series of Regional Webinars, GLACY+
- 8 December, C-PROC, (on-line), Joint Workshop on International Cooperation in Cybercrime and Electronic Evidence co-organised with EUROJUST, GLACY+, iPROCEEDS-2, CyberSouth, CyberEast
- 8-9 December, C-PROC/Netherlands, (on-line), Regional Meeting on international cooperation and MLA step-by step guidelines (in cooperation with Eurojust), CyberEast
- 8 - 9 December, C-PROC/Kiribati, (on-line), Advisory workshop on cybercrime and electronic evidence legislation, GLACY+
- 8 - 11 December, C-PROC, (on-line), Pilot training on online child sexual abuse and exploitation for judges, prosecutors and the national police, EndOCSEA@Europe, CyberEast

- 9 - 11 December, C-PROC, (on-line), Online workshop on improving information sharing and cooperation between CERT and LEA in Republika Srpska, iPROCEEDS-29 December, C-PROC/Lebanon, (on-line), Second national meeting on the development of domestic Standard Operating Procedures and a toolkit for first responders on cybercrime investigation and e-evidence, CyberSouth
- 10 December, C-PROC, (on-line), CyberSouth Project Steering Committee, CyberSouth
- 10 December, T-CY, Information meeting on Cybercrime, Organised by the Thematic Coordinator on Information Policy (TC-INF), the Chair of the Rapporteur Group on Legal Cooperation (GR-J) and the Cybercrime Division of the Council of Europe
- 11 December, C-PROC, (on-line) 3rd Working Group meeting on the development of the on-line training platform, Cybercrime@Octopus, GLACY+, iPROCEEDS-2, CyberSouth, CyberEast
- 14-16 December, C-PROC/Ukraine, (on-line), Effective access to data exercise and development of standard procedures between LEA/ISPs, CyberEast
- 14 - 16 December, C-PROC/Gambia (on-line), Support for drafting the Data Protection Law, in collaboration with the Data Protection Unit of the Council of Europe, GLACY+
- 14 December [TBC], Working Group meeting for development of the HELP course on Cybercrime, Cybercrime@Octopus, GLACY+, iPROCEEDS-2, CyberSouth, CyberEast
- 16 December, C-PROC, (on-line), 4th Working Group meeting on the development of the on-line training platform, Cybercrime@Octopus, GLACY+, iPROCEEDS-2, CyberSouth, 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 November 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