Cybercrime Digest

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

16 – 30 June 2021

Source: Council of Europe

Date: 28 - 29 June 2021

Second African Forum on cybercrime: creating synergies for a coordinated approach to protect societies from the threat of cybercrime

"Following the success of the First African Forum on cybercrime, the African Union Commission, the European Union and the Council of Europe (GLACY+ and Octopus Project), in partnership with other international Organisations, hosted the Second continent-wide African Forum on Cybercrime. The event took place online between 28-29 June 2021, bringing together more than 300 delegates from across the continent on each day – policy makers and legislators, representatives from the criminal justice sector (prosecutors, judges, law enforcement), delegates from ministries responsible for the implementation of cybercrime and cybersecurity policies, and other national and international stakeholders with an active role in the cybercrime domain." READ MORE

Source: Council of Europe

Date: 28 June 2021

Save the date: Octopus Conference 2021!

"This year's Octopus Conference will take place on 16-18 November providing an opportunity for cybercrime experts from public and private sectors as well as international and non-governmental organizations from all over the world to share experience. A special event with high level interventions will be organized on 16 November in cooperation with the Hungarian Chairmanship of the Committee of Ministers on the occasion of the 20th anniversary of the Budapest Convention and the 2nd additional Protocol on enhanced cooperation and disclosure of electronic evidence." READ MORE

Source: Council of Europe

Date: 17 June 2021

Closing Conference of the EndOCSEA@Europe project

"EndOCSEA@Europe project held the closing conference as part of Together to #ENDviolence and affiliate event of the Solutions Summit Series, by organising three webinars on Fighting online child sexual exploitation and abuse with new standards and policies, research, knowledge and awareness raising tools." READ MORE

Source: Centr

Date: 18 June 2021

ICANN71: Data accuracy obligation and EPDP - what's next?

"Three years after the EU GDPR entered into force, the ICANN community is still debating the emergency measures with regard to data protection of gTLD registration data. Before the GDPR, gTLD registration data was publicly available, but the accuracy of this data is an issue that the community was facing long before that. In 2021, the Expedited Policy Development Process (EPDP) moved on to Phase 2A, with one main issue in focus: the distinction between natural and legal persons in the domain name registration process." READ MORE

RELATED ARTICLE:

Centr, ICANN71 and DNS Abuse, 17 June 2021

Source: EUROPOL

Date: 30 June 2021

Coordinated action cuts off access to VPN service used by ransomware groups

"This week, law enforcement and judicial authorities in Europe, the US and Canada have seized the web domains and server infrastructure of DoubleVPN. This is a virtual private network (VPN) service which provided a safe haven for cybercriminals to attack their victims. Servers were seized across the world where DoubleVPN had hosted content, and the web domains were replaced with a law enforcement splash page. This coordinated takedown was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). […] International cooperation was central to the success of this investigation as the critical infrastructure was scattered across the world." READ MORE

Source: Security Boulevard

Date: 28 June 2021

EU, U.S. Partner on Malware, Cybersecurity Defense

"[…] When it comes to bilateral and multilateral instruments to facilitate the fight against cybercrime, the United States and the European Union restated their commitment to negotiate as soon as possible an EU-U.S. agreement facilitating access to electronic and digital evidence for the purpose of cooperation in criminal matters. Both sides also welcomed the recent approval by the Committee of State Parties to the Budapest Convention of the draft text of the Second Additional Protocol of the Budapest Convention, which remains the primary instrument for international cooperation on cybercrime." READ MORE

RELATED ARTICLE:

Público, UE e EUA criam grupo de trabalho para combater cibercrime, 22 June 2021

Source: Council of Europe

Date: 25 June 2021

Automated Detection of Online Child Sexual Exploitation and Sexual Abuse. Findings and recommendations

"The scale of online child sexual exploitation and abuse is increasing at an alarming rate. To date, the response to this challenge consists also of voluntary actions involving the use of automated detection technologies by private sector actors to detect, report and remove child sexual abuse materials. While this is vital to help rescue child victims, investigate crimes and stop circulation of abuse material, the use of automated technology may impact on the confidentiality of communications that service providers must ensure. […] States have a positive obligation to protect children from sexual abuse and exploitation. To do so, they must however take into account a complex and evolving environment both from technological and legal points of view." READ MORE

Source: BBC

Date: 21 June 2021

The Lazarus heist: How North Korea almost pulled off a billion-dollar hack

"In January 2015, an innocuous-looking email had been sent to several Bangladesh Bank employees. It came from a job seeker calling himself Rasel Ahlam. His polite enquiry included an invitation to download his CV and cover letter from a website. In reality, Rasel did not exist - he was simply a cover name being used by the Lazarus Group, according to FBI investigators. At least one person inside the bank fell for the trick, downloaded the documents, and got infected with the viruses hidden inside." READ MORE, VERSION FRANÇAISE

Source: The Conversation

Date: 18 June 2021

Inside a ransomware attack: how dark webs of cybercriminals collaborate to pull them off

"The problem for law enforcement is that ransomware – a form of malware used to steal organisations' data and hold it to ransom – is a very slippery fish. Not only is it a blended crime, including different offences across different bodies of law, but it's also a crime that straddles the remit of different policing agencies and, in many cases, countries. And there is no one key offender. Ransomware attacks involve a distributed network of different cybercriminals, often unknown to each other to reduce the risk of arrest. " READ MORE

Source: Business Ghana

Date: 1 July 2021

Ghana ranked Africa's third in cybersecurity

"Ghana scored 86.69 per cent for secure cyberspace and comes behind Mauritius and Tanzania in that order. Ghana's new ranking in Africa is a major leap from the 11th position attained in the previous rating of 32.6 per cent in 2017 and 43.7 per cent in 2018, projecting the country among the best in the region and globally. The current assessment covers the 2019-2020 period and reflects data collected during the COVID-19 pandemic. […]Commenting on the rankings released last Tuesday by the world telecommunications governing body, the National Cybersecurity Advisor, Dr Albert Antwi-Boasiako, said the achievement was proof of the government's commitment to develop the country's cyberspace for a sustained digital transformation in a secure and resilient manner." READ MORE

Source: SwitSalone

Date: 25 June 2021

Parliament of Sierra Leone enacts the Cyber Crime Bill

"The Parliament of Sierra Leone has on Wednesday, June 23, 2021, passed the Cyber Crime Bill into law, titled "The Cyber Security and Crime Act 2021". The act which is introduced in Sierra Leone for the first time will provide prevention on the abusive use of computers, and provide a timely and effective collection of electronic evidence for investigation and prosecution of cybercrime. It will also protect critical national information infrastructure, promote cybersecurity, protect computer programs, intellectual property and privacy rights." READ MORE

RELATED ARTICLE:

Sierra Leone Telegraph, Sierra Leone's Cyber Security and Crime Bill: An organized opposition makes democracy work well, 24 June 2021

Source: All Africa

Date: 28 June 2021

Morocco: Personal Data - Morocco, Burkina Faso Strengthen Their Cooperation

"The National Commission for the Supervision of Personal Data Protection (CNDP) and the Commission of Informatics and Liberties (CIL) of Burkina Faso signed, on Monday in Rabat, a cooperation protocol on the establishment of a bilateral mechanism of collaboration. Under this protocol, inked by CNDP president Omar Seghrouchni and CIL head Marguerite Ouedraogo Bonane, both parties are jointly committed to ensuring the best possible protection of personal data. […] Marguerite Ouedraogo Bonane stressed that the agreement provides for the usual actions that the two authorities carry out in the field, including those related to information, awareness and management of complaints from victims of cybercrime." READ MORE

Source: Council of Europe

Date: 15 & 16 June 2021

CyberSouth: National Workshop for judges, prosecutors and law enforcement on the application of data protection requirements in Algeria and Tunisia

The series of National Workshops for judges, prosecutors and law enforcement on the application of data protection requirements continued with the last meeting, on the 15th and 16th of June, for the Algerian and Tunisian representatives' benefit. Convention 108+ for the protection of individuals with regard to automated processing of personal data, its international legal standards and principles, was presented, together with the findings of the studies drafted under the framework of CyberSouth project. READ MORE HERE and HERE

Source: India Today

Date: 18 June 2021

India: Government launches national helpline for cyber fraud, here is how it works

"The Union Home Ministry has operationalised the national helpline 155260 and reporting platform for preventing financial loss due to cyber fraud. […] The government has noted that the helpline will be rolled out in all states of India and is operated by the state police. The helpline which was soft-launched on April 2021 and has been made operational by the Indian Cyber Crime Coordination Centre (I4C), with active support and cooperation from the Reserve Bank of India (RBI), all major banks, payment banks, wallets and online merchants." READ MORE

RELATED ARTICLE:

Bank Info Security, India Launches Effort to Track, Freeze Cyber Fraud Proceeds, 21 June 2021

Source: Council of Europe

Date: 25 June 2021

GLACY+: Workshop on a new cybercrime act in Tonga

"Party to the Budapest Convention and GLACY+ priority country since 2017, Tonga has adopted in November 2020 the Electronic Communication Abuse Act 2020 […] , introducing obligations for service providers to assist LEA and the mandatory production order for access to data. […] further amendments of the legislation on cybercrime and electronic evidence are pending with the Tongan Parliament. GLACY+ project supported the Attorney General Office of Tonga in organizing a hybrid workshop on June 24-25, with the aim of fully preparing stakeholders into implementing the new cybercrime provisions in practice." READ MORE

Source: Council of Europe

Date: 11 June 2021

GLACY+: Strong commitment of the PNG authorities for the accession to Budapest Convention

"The GLACY+ Project supported the organization of two back-to-back events in Papua New Guinea. The Online Introductory Training Course on Cybercrime and Electronic Evidence for Judges was organized in collaboration with the Papua New Guinea Centre for Judicial Excellence (PNGCJE) on 8 and 9 June, followed by the Workshop on Cybercrime Legislation and Criminal Justice Capacities, held in a hybrid format and co-organized with the Department of Justice & Attorney General and PNGCJE on 10 and 11 June." READ MORE

Source: Intelligent CIO

Date: 18 June 2021

Survey reveals Latin America's cybercrime map

"According to a survey by F5 Networks, Brazil is in seventh place in the ranking of cybercrimes with seven million attacks, while Argentina is in ninth place, with six million criminal actions. In addition, the study reveals that in the pandemic era, cybercriminals continue to scan remote access ports to break into businesses and governments." READ MORE

RELATED ARTICLE:

F5 Labs, Cyberattacks Targeting Latin America, January through March 2021, 28 June 2021

Source: Cámara de Diputados

Date: 14 June 2021

Insta Raúl Bonifaz a la SRE para que México se adhiera al Convenio de Budapest, en materia de ciberseguridad

"Ante este panorama, Bonifaz Moedano consideró que es imperante ratificar el Convenio sobre la Ciberseguridad del Consejo de Europa, dado que es el "acuerdo internacional de uso más extendido para desarrollar la legislación de combate al cibercrimen." Puntualizó que el tratado ha sido ratificado por 60 Estados de la Unión Europea, así como algunos exteriores como Canadá, Estados Unidos, Australia y Japón. Recordó que el convenio fue emitido el 23 de noviembre de 2001, y se "trata del único tratado internacional vinculante en la materia y constituye una especie de guía, "ley modelo" o "acuerdo marco"." READ MORE

RELATED ARTICLE:

Zacatecas, Urgente, legislar en materia de ciberseguridad: expertos, 25 June 2021

Source: Canadian Government

Date: 23 June 2021

Government of Canada takes action to protect Canadians against hate speech and hate crimes

"This bill will be complemented by a regulatory framework to tackle harmful content online. In the coming weeks, the Government of Canada will engage Canadians on a detailed technical discussion paper that will outline the proposal for making social media platform operators more transparent and accountable while combating harmful content online." READ MORE

Source: FCW

Date: 17 June 2021

New bill looks to ramp up penalties for ransomware crooks

"The bill permits law enforcement to seize funds generated from the sale of spyware and to take equipment such as illegal intercept devices used in the commission of hacking campaigns, ransomware and other nefarious activity, according to a fact sheet provided by the lawmakers. The bill would also make it easier for DOJ to go after botnets by expanding the list of reasons the federal government can seek injunctive relief. Under the current law, DOJ can only seek relief when a botnet is engaged in fraud or illegal wiretapping. The new bill would broaden that activity to include the destruction of data, denial of service attacks and certain violations in the Computer Fraud and Abuse Act." READ MORE

RELATED ARTICLE:

International Cybercrime Prevention Act of 2021, 17 June 2021

Source: POLITICO

Date: 21 June 2021

EU to launch rapid response cybersecurity team

"The European Union wants to launch a new cyber unit to respond to cyberattacks, according to a draft of the plan seen by POLITICO. The European Commission will present its plan on Wednesday to set up what it calls the "Joint Cyber Unit," which would allow national capitals hit by cyberattacks to ask for help from other countries and the EU, including through rapid response teams that can swoop in and fight off hackers in real time, according to the draft. […] The EU's plan aims to help countries fight back against increasingly sophisticated and brash attacks by pooling national governments' cybersecurity powers." READ MORE

RELATED ARTICLE:

European Council/Council of the EU, Cybersecurity: how the EU tackles cyber threats, 23 June 2021

Source: Organized Crime and Corruption Reporting Project

Date: 16 June 2021

Italy to Launch Government Agency to Counter Cybercrime

"[…] The cabinet-approved decree-law includes "urgent provisions on cybersecurity" in Italy and the creation of a National Cybersecurity Agency as part of a national cyber-resilience strategy that seeks to raise the populations' awareness on matters related to cyber threats, authorities said in a statement. The unit, which falls under the Prime Minister's responsibility, will be in charge of developing national capabilities for preventing, monitoring, detecting and mitigating cyber attacks in cooperation with other Italian agencies." READ MORE

Latest reports

- Europol, The Cyber Blue Line, 25 June 2021
- Europol, Consolidated Annual Activity Report (Caar) 2020, 22 June 2021
- CEPOL, Sirius e-evidence series – now available on leed in French, Italian and Spanish, 28 June 2021
- ENISA, Cybersecurity for SMEs - Challenges and Recommendations, 28 June 2021
- ENISA, Phishing most common Cyber Incident faced by SMEs, 28 June 2021
- ENISA, How to Help National Authorities deal with the Challenges of Mobile Networks Security?, 22 June 2021
- UNODC, UNODC World Drug Report 2021: pandemic effects ramp up drug risks, as youth underestimate cannabis dangers, 24 June 2021
- Krebs on security, How Cyber Safe is Your Drinking Water Supply?, 21 June 2021
- Schneier on security, Banning Surveillance-Based Advertising, 24 June 2021
- BBC, The Lazarus Heist (Podcast), June 2021
- Tech Monitor, The top ten ransomware gangs, 28 June 2021
- Bank Info Security, Law Enforcement's Cybercrime Honeypot Maneuvers Paying Off, 18 June 2021

Upcoming events

- 1-2 July, C-PROC/GEORGIA, (on-line), National training for cybercrime units and prosecutors on use of templates for data preservation and subscriber information, CyberEast
- 2 July, C-PROC/MAURITIUS, (on-line), Workshop on the new cybercrime legislation in Mauritius, GLACY+
- 2 July, C-PROC, (on-line), 3rd Webinar to address issues and challenges for chapters 5-10 of the Python Programming for Investigators, iPROCEEDS-2
- 5 July, C-PROC/BURKINA FASO, BENIN, MOROCCO, SENEGAL, Workshop on LEA training strategies, GLACY+
- 5-6 July, C-PROC/MOLDOVA, (on-line), National training for cybercrime units and prosecutors on use of templates for data preservation and subscriber information, CyberEast
- 5-8 July, C-PROC/WESTERN AFRICAN COUNTRIES, (on-line), Introductory Judicial Training on Cybercrime and Electronic Evidence for English speaking countries, in collaboration with OCWAR-C Project, GLACY+
- 6 July, C-PROC/AFRICA, Regional HUB to the Second African Forum - Southern Africa Hub on Specialized Units, GLACY+
- 6 July, C-PROC/BENIN, (on-line), Advisory mission on LEA training strategies and integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, GLACY+
- 7 July, C-PROC/TURKEY, (on-line), 2nd delivery of the Workshop on acquisition of regular/digital evidence in cybercrime cases, for Turkish magistrates. Investigating, prosecuting and adjudicating cybercrime offences and relevant evidence, iPROCEEDS-2
- 7 July, C-PROC/BURKINA FASO, (on-line), Advisory mission on LEA training strategies and integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, GLACY+

- 7 July, C-PROC/BURKINA FASO, (on-line), Advisory mission on legislation, GLACY+
- 7 July, C-PROC/ARMENIA, (on-line), Workshop with Armenian authorities on cybercrime/ cybersecurity strategy and action plan, in cooperation with CyberSecurity EAST Project, CyberEast
- 7 July, C-PROC/ARMENIA, (on-line), Workshop with Armenian authorities on the reform of criminal procedure legislation, CyberEast
- 8 July, C-PROC, (on-line), 6th Steering Committee meeting of the project, CyberSouth
- 8 July, C-PROC/LATAM, (on-line), Workshop for Cybercrime Units, in collaboration with EL PAcCTO project, GLACY+8 July, C-PROC, (on-line), Series of monthly thematic webinars for the International Network of the National Judicial Trainers (6/7), GLACY+
- 8 July, C-PROC/MOROCCO, (on-line), Advisory mission on LEA training strategies and integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, GLACY+
- 8-9 July, C-PROC/UKRAINE, (on-line), National training for cybercrime units and prosecutors on use of templates for data preservation and subscriber information, CyberEast
- 9 July, C-PROC/ SENEGAL, (on-line), Advisory mission on LEA training strategies and integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, GLACY+
- 9 July, C-PROC/ LEBANON, (desk review), Law Enforcement Training strategy, CyberSouth
- 12 July, C-PROC, (on-line), 10th Steering Committee meeting of the project, GLACY+
- 12-14 July, C-PROC/AZERBAIJAN, (on-line), Effective access to data exercise and development of standard procedures between LEA/ISPs, CyberEast
- 12-15 July C-PROC/WESTERN AFRICAN COUNTRIES, (on-line), Introductory Judicial Training on Cybercrime and Electronic Evidence for FR speaking countries, in collaboration with OCWAR-C, GLACY+
- 13 July, C-PROC/AFRICA, (on-line), Series of regional webinars to Promote Universality and Implementation of the Budapest Convention on Cybercrime (1/4), GLACY+, Octopus
- 13 July, C-PROC/TUNISIA, (on-line), Advisory workshop on establishing the 24/7 contact point, CyberSouth
- 15 July, C-PROC/COTE D'IVOIRE, (on-line), Advisory mission on legislation, GLACY+
- 15 July, C-PROC, (on-line), Workshop on the Digital Forensic/Triage/Live Data forensic tools developed by UCD within the FREETOOL Project, iPROCEEDS-2

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 July 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