Cybercrime Digest

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

1 – 15 June 2021

Source: Global Initiative

Date: 2 June 2021

Contested domain: UN cybercrime resolution stumbles out of the gate

"On 26 May 2021, a resolution on cybercrime was voted through the United Nations General Assembly. The General Assembly took place in the wake of two major cyber incidents, providing timely evidence of the need for a response. This resolution was mainly organizational, determining the rules and process to debate and possibly draft a treaty 'on countering the use of information and communications technologies for criminal purposes', but was subject to strong disagreement among member states, with serious doubt as to whether progress was possible." READ MORE

RELATED ARTICLE:

Technology and Business, UN takes new step towards international cybercrime laws – a blow for online freedoms?, 3 June 2021

Source: Europol

Date: 8 June 2021

800 criminals arrested in biggest ever law enforcement operation against encrypted communication

"The US Federal Bureau of Investigation (FBI), the Dutch National Police (Politie), and the Swedish Police Authority (Polisen), in cooperation with the US Drug Enforcement Administration (DEA) and 16 other countries have carried out with the support of Europol one of the largest and most sophisticated law enforcement operations to date in the fight against encrypted criminal activities." READ MORE

Source: US Department of Justice

Date: 7 June 2021

Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside

"The Department of Justice today announced that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation." READ MORE

RELATED ARTICLE:

Malwarebytes Lab, DOJ recovers pipeline ransom, signals more aggressive approach to cybercrime, 8 Jun 2021

Source: Bahia.ba

Date: 14 June 2021

Câmara discute adesão do Brasil à convenção de crimes cibernéticos

"A Comissão de Relações Exteriores da Câmara dos Deputados promoveu audiência pública nesta segunda-feira (14) para avaliar a proposta de adesão do Brasil à Convenção sobre o Cibercrime, também chamada de Convenção de Budapeste, em referência ao local de assinatura, em 2001. A convenção recebeu até o momento a adesão de 66 países." READ MORE

Source: Mipuntodevista

Date: 14 June 2021

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

"El diputado Raúl Eduardo Bonifaz Moedano (Morena) promueve un punto de acuerdo que presentó ante la Comisión Permanente, para que la Secretaría de Relaciones Exteriores (SRE) adhiera y ratifique a México en el Convenio de Ciberdelincuencia, también llamado Convenio de Budapest y su Protocolo Adicional, en materia de ciberseguridad." READ MORE

Source: US Department of Justice

Date: 10 June 2021

Slilpp Marketplace Disrupted in International Cyber Operation

"The Justice Department today announced its participation in a multinational operation involving actions in the United States, Germany, the Netherlands, and Romania to disrupt and take down the infrastructure of the online marketplace known as Slilpp. According to the affidavit, the FBI, working in coordination with foreign law enforcement partners, identified a series of servers that hosted the Slilpp marketplace infrastructure and its various domain names. Those servers and domain names were seized pursuant to domestic and international legal process." READ MORE

Source: US Department of Justice

Date: 7 June 2021

Four Individuals Plead Guilty to RICO Conspiracy Involving "Bulletproof Hosting" for Cybercriminals

"[…] Over the course of many years, the defendants facilitated the transnational criminal activity of a vast network of cybercriminals throughout the world by providing them a safe-haven to anonymize their criminal activity," said Special Agent in Charge Timothy Waters of the FBI's Detroit Field Office.[…] The FBI investigated the case with critical assistance from law enforcement partners in Germany, Estonia, and the United Kingdom." READ MORE

Source: lemonde.fr

Date: 9 June 2021

Cybersécurité : l'Afrique sous la menace d'un « chaos numérique

"Un « chaos numérique ». Telle est la menace qui plane sur une Afrique de plus en plus interconnectée mais en retard dans le domaine de la sécurité informatique. Ce constat alarmant faisait l'unanimité parmi les participants du premier Cyber Africa Forum, un événement rassemblant des experts de la cybersécurité africains et internationaux, lundi 7 juin à Abidjan." READ MORE

Source: Allaafrica.com

Date: 9 June 2021

South Africa Lays Down the Law On Cybercrime

"A new law brings South Africa up to international standards for fighting cybercrime. With a global spike in internet-based offences, partly driven by more people working from home due to the COVID-19 pandemic, it couldn't come soon enough. The country's well-developed financial infrastructure makes it an attractive target for cyber criminals who use the internet for extortion, fraud, child pornography, human trafficking and selling illicit goods.[…] Together with the Protection of Personal Information (POPI) Act 2020, […] the new cyber law is a key part of South Africa's armory in the fight against cybercrime." READ MORE

Source: Thisdaylive.com

Date: 3 June 2021

Nigeria : Operators Warn against Cybercrime

"The Nigeria Computer Society (NCS), the umbrella body for Information Technology (IT) practitioners in Nigeria, has expressed concern over the increasing rate of cyber-security challenges in the country. To this end, the group has advised government and the private sector on new measures to nip the development in the bud. NCS gave the new measures during its second stakeholders' forum on cyber-security, which held recently in Abuja." READ MORE

Source: Council of Europe

Date: 7 June 2021

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

"The series of National Workshops for judges, prosecutors and law enforcement on the application of data protection requirements in the priority countries continued with the second meeting, on the 7th of June 2021, for Moroccan representatives. Convention 108+ for the protection of individuals with regard to the processing of personal data was presented in terms of international legal standards and principles." READ MORE

Source: Council of Europe

Date: 9 June 2021

EndOCSEA@Europe & Cyber East: Improving operational capacities to tackle online child sexual exploitation and abuse

"The Council of Europe Project to End Online Child Sexual Exploitation and Abuse@Europe (EndOCSEA@Europe) launched its new training package for law enforcement, judges and prosecutors to improve their operational capacities in tackling OCSEA in an online Regional Conference on 3-4 June 2021. […] it was done in its piloting at country level throughout the project in cooperation with national experts from Ukraine, Republic of Moldova and Georgia." READ MORE

Source: EUfordigital.eu

Date: 7 June 2021

Cyberspace: EU and Ukraine launch dialogue on cyber security

"The European Union and Ukraine have held their first cyber dialogue, in a meeting on 3 June. The EU and Ukraine reaffirmed their commitment to a global, open, stable and secure cyberspace, where the rule of law is fully respected, where the same rights that individuals have offline are also protected online, and where the security, economic growth, prosperity, and integrity of free and democratic societies is promoted and preserved." READ MORE

Source: zdnet.com

Date: 2 June 2021

Russian underground forums launch competitions for cryptocurrency, NFT hacks

"Over the past month, according to Intel 471, operators of Russian underground forums have been running a competition asking for papers that examine "how to target cryptocurrency-related technology." Starting April 20, the contest requests unorthodox methods covering everything from the theft of private keys and wallets used to store cryptocurrency including Bitcoin (BTC) and Ethereum (ETH) to submissions for "unusual" cryptocurrency mining software, as well as proposals relating to smart contracts and non-fungible tokens (NFTs)." READ MORE

Source: US Department of Justice

Date: 4 June 2021

Latvian National Charged for Alleged Role in Transnational Cybercrime Organization

"A Latvian national was arraigned in federal court in Cleveland, Ohio, today on multiple charges stemming from her alleged role in a transnational cybercrime organization responsible for creating and deploying a computer banking trojan and ransomware suite of malware known as "Trickbot. […] The Trickbot Group operated in Russia, Belarus, Ukraine, and Suriname, and primarily targeted victim computers belonging to businesses, entities, and individuals, including those in the Northern District of Ohio and elsewhere in the United States." READ MORE

Source: Council of Europe

Date: 8 June 2021

GLACY+: Online stakeholder webinar on new cybercrime legislation in Belize

"Further to the launch of the National Cybersecurity Strategy for the years 2020-2023 and the enactment of the Cybercrime Act by the House of Representatives of Belize from September 2020, on 3 June 2021, the Council of Europe, through the GLACY+ project, in collaboration with the Ministry of Home Affairs of Belize, organized an online workshop focused on the access of criminal justice authorities to data held by private parties and roles and responsibilities for on-line service providers in the light of the provisions of the Cybercrime Act." READ MORE

Source: Manila Times

Date: 4 June 2021

Philippines: Resurgent ransomware threatens cyber systems

"Ransomware, a cybercrime that encrypts systems and locks their owners out until a ransom is paid, has resurfaced globally, and attacks on Philippine cyber firms are likely to increase. Just last May, a ransomware attack affected a subsidiary of the French insurance company Axa, impacting operations in numerous Asian nations, including the Philippines. READ MORE

Source: Reuters

Date: 10 June 2021

In a world first, El Salvador makes bitcoin legal tender

"El Salvador became the first country in the world to adopt bitcoin as legal tender after Congress on Wednesday approved President Nayib Bukele's proposal to embrace the cryptocurrency, a move that delighted the currency's supporters. With 62 out of 84 possible votes, lawmakers voted in favour of the move to create a law to adopt bitcoin, despite concern about the potential impact on El Salvador's program with the International Monetary Fund." READ MORE

Source: publicsenat.fr

Date: 10 June 2021

Cyberattaques: le Sénat préconise d'interdire le paiement par les assurances des rançongiciels

"La délégation aux entreprises du Sénat présentait, ce jeudi, une vingtaine de propositions afin de prévenir les cyberattaques visant les TPE et PME françaises. Près de la moitié d'entre elles a été visée l'année dernière. […] En 2020, 43 % des PME françaises ont constaté un incident de cybercriminalité en 2020 pour un préjudice allant de plusieurs milliers d'euros à plusieurs millions d'euros en fonction de la taille des entreprises." READ MORE

Source: Euractiv

Date: 2 June 2021

Cloud development in Europe passes by GDPR compliance

"The two recently approved Codes of Conduct for the cloud industry, which will be open to everyone willing to subscribe, could foster the uptake of a technology at the heart of the digital economy, following a green light from the European Data Protection Board. The two Codes have been developed by industry leaders to provide a blueprint for compliance with the EU's data protection regulation, the GDPR, in a cloud environment and are the first of their kind to be formally approved by the European data protection authorities." READ MORE

Source: Council of Europe

Date: 11 June 2021

European ministers adopt priority actions to enhance journalists' safety and address AI's impact on freedom of expression

"European Ministers responsible for Media and Information Society have agreed to carry out a number of priority actions to tackle the most pressing challenges to freedom of expression, including the decline in the safety of journalists and the impact of Artificial Intelligence (AI) and of massive digitalisation in the media and information environments on freedom of expression. At the conclusion of a Council of Europe Ministerial Conference held on 10 and 11 June, the Ministers adopted a Final Declaration and four resolutions covering areas where the Council of Europe will focus its efforts to protect freedom of expression in the next years: digital technologies, safety of journalists, the changing media and information environment, and the impact of the Covid-19 pandemic on freedom of expression." READ MORE

Latest reports

- Australian Human Rights Commission, Human Rights and Technology final report, 27 May 2021
- Facebook, Threat Report, The State of Influence Operations 2017-2020, 1 June 2021
- Feedzai, Q2 2021 Financial Crime Report: The Dollar Takes Flight, 2 June 2021
- ENISA, New Light Shed on Capabilities in Energy & Healthcare, 3 June 2021
- Security Affairs, The dark web index 2021 report, 4 June 2021
- Beta Shares, Making cybercrime pay: the growth opportunity in cybersecurity, 4 June 2021
- Databasix, 20 Frightening Cyber Security Facts and Stats, 7 June 2021
- Euractiv, What Are GDPR's Hidden Benefits Three Years On?, 9 June 2021
- ESET, BackdoorDiplomacy: Upgrading from Quarian to Turian, 10 June 2021
- Australian Government, The Commonwealth Cyber Security Posture in 2020, 10 June 2021

Upcoming events

- 14-17 June, C-PROC/NETHERLANDS, (on-line), ICANN 71 meeting, GLACY+
- 16 June, C-PROC/TUNISIA, (on-line), In-country workshop for judges, prosecutors and law enforcement on the application of cybercrime legislation, including rule of law safeguards and data protection requirements, CyberSouth
- 16 June, C-PROC, (on-line), Second webinar to address issues and challenges for chapters 1-5 of the Python Programming for Investigators Online Course, iPROCEEDS-2, GLACY+, CyberEast, CyberSouth, Octopus
- 17 June, C-PROC/Children's Rights Division, (on-line), Closing Conference od the project: Fighting OCSEA with new standards and policies, research, knowledge and awareness raising tools, EndOCSEA@Europe
- 18 June, C-PROC/LEBANON, Desk study, Support the development of the Law Enforcement Training Strategy, CyberSouth
- 18 June, C-PROC/Children's Rights Division, (on-line), Final Steering Committee meeting, EndOCSEA@Europe
- 22 June, C-PROC/AFRICA, (on-line), General Assembly of the African Network of DPAs, GLACY+
- 22 June, C-PROC (on-line), Series of monthly thematic webinars for the International Network of the National Judicial Trainers (6/7), GLACY+
- 22-24 June, C-PROC/ KOSOVO* (on-line), Specialised Judicial Training Course on International Cooperation, iPROCEEDS-2
- 23-25 June, C-PROC/MOLDOVA, (on-line), Pilot session of online judicial training, CyberEast
- 28 June - 3 July, C-PROC/SENEGAL, (on-line), Regional Training of Trainers for Gendarmerie of Francophone countries from Africa, GLACY+
- 28-30 June, C-PROC/AZERBAIJAN, (on-line), Effective access to data exercise and development of standard procedures between LEA/ISPs, CyberEast
- 28-30 June, C-PROC, (on-line), Contribution to EuroDIG 2021, CyberEast
- 28-30 June, C-PROC/ ETHIOPIA, (on-line), Second African Forum on Cybercrime, co-organized with the African Union, GLACY+, Octopus

- 29 June, C-PROC, (on-line), Regional online meeting with all project countries/area on MLA best practices as provided under the Budapest Convention and as further enhanced under its Second Additional Protocol, iPROCEEDS-2
- 30 June, C-PROC/ TURKEY (on-line), First 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

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 June 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