Cybercrime Digest

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

16 – 31 March 2021

Source: Council of Europe

Date: 29 Mar 2021

The Riksdag of Sweden approves ratification of the Budapest Convention on Cybercrime

"The Riksdag of Sweden approved ratification of the Budapest Convention on Cybercrime, as well as of its Additional Protocol on Xenophobia and Racism committed through computer systems. This will allow the Government of Sweden to deposit the instrument of ratification at the Council of Europe and to become a Party to these treaties in the very near future." READ MORE

Source: CyberPeace Institute

Date: 23 Mar 2021

Civil Society Voices Must be Heard in the UN Cybercrime Convention Process

"A new process to negotiate an international convention to counter cybercrime is due to start in May 2021 in the Third Committee of the United Nations General Assembly. The Resolution 74/247 adopted by the General Assembly in December 2019 established an open-ended ad hoc intergovernmental committee of experts, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Their first meeting, scheduled for May 2021, will discuss the working modalities for the ad-hoc committee hosted by the UN Office for Drugs and Crime." READ MORE

Source: Council of Europe

Date: 24 – 26 Mar 2021

GLACY+ welcomes Colombia as a priority country

"The GLACY+ Project, together with INTERPOL, supported the Ministry of Foreign Affairs in Colombia in organizing a three-day workshop with the scope of assessing the current state of the cybercrime legislation and identifying the capacity building needs in Colombia. […] A national coordination team soon to be set up will work closely with the GLACY+ project to include Colombia among its priority countries and shape an action plan for reinforcing institutional capacities in the cooperation against cybercrime." READ MORE

Source: Council of Europe

Date: 24 – 26 Mar 2021

MPF participa de workshop para implementação da Ação Global Alargada contra o Cibercrime

"Programa Glacy+ visa fortalecer a capacidade dos países para aplicar a Convenção de Budapeste, único tratado internacional sobre crime cibernético e evidências eletrônicas. O Ministério Publico Federal (MPF) participou, nesta quarta-feira (24), de workshop do Projeto GLACY+ (Ação Global Alargada contra o Cibercrime). Trata-se de iniciativa conjunta, co-financiada pela União Europeia e pelo Conselho da Europa, destinada fortalecer a capacidade dos países para aplicar a Convenção de Budapeste, único tratado internacional sobre crime cibernético e evidências eletrônicas. A iniciativa visa ainda o aprimoramento de técnicas de cooperação internacional eficaz nessa área." READ MORE

RELATED ARTICLE:

Council of Europe , GLACY+: Brazil is a new Priority Country, 24-26 March 2021

Source: Interpol

Date: 24 Mar 2021

Online vaccine scams: INTERPOL and Homeland Security Investigations issue public warning - 'Be vigilant, be skeptical, be safe'

"INTERPOL and the United States' Homeland Security Investigations (HSI) have joined forces to warn the public against purchasing alleged COVID-19 vaccines and treatments online. […] "From the very beginning of the pandemic, criminals have preyed on people's fears in order to make fast cash. Fake vaccines are the latest in these scams, which is why INTERPOL and HSI are warning the public to be extra vigilant," said INTERPOL Secretary General Jürgen Stock." READ MORE

Source: The Washington Post

Date: 31 Mar 2021

Opinion: How Russia and China are attempting to rewrite cyberworld order

"Many people have grown used to thinking of the United Nations in recent decades as an annoying talk shop, created with the noblest intentions but increasingly a morass of bureaucracy and mutual back-scratching. But for China and Russia, the United Nations is increasingly the venue for unsubtle power plays — often ignored by the United States — that could shape the new world order that's emerging. […] Cyberspace is the best example of a domain where authoritarian nations, led by China and Russia, are using the United Nations to craft new rules that could undermine Western norms of openness and democracy." READ MORE

Source: US Department of Treasury

Date: 19 Mar 2021

Foreign Nationals Sentenced for Roles in Transnational Cybercrime Enterprise

"The Infraud Organization victimized millions of people in all 50 states and caused more than $568 million in financial losses.

Two foreign nationals — one Russian, the other Macedonian — were sentenced today for their role in the Infraud Organization, a transnational cybercrime enterprise engaged in the mass acquisition and sale of fraud-related goods and services, including stolen identities, compromised credit card data, computer malware, and other contraband." READ MORE

Source: The Southern Times Africa

Date: 29 Mar 2021

Zambia: President Lungu signs Cybercrime Law

"Zambian President Edgar Lungu has signed the Cyber Security and Cyber Crimes Bill of 2021 into law […].The Cyber Security and Cyber Crimes Act provides for collection and preservation of computer and network related crime, as well as revise the admission in criminal matters of electronic evidence. It provides for registration of cyber security service providers and for matters connected with, or incidental to, the foregoing." READ MORE

Source: The Cable

Date: 18 Mar 2021

Nigeria ranked 16th in FBI global cybercrime victims report

"In its latest internet crime report, FBI said Nigeria received 443 complaints relating to internet crime last year. The top five crimes reported include phishing, non-payment/non-delivery, extortion, personal data breach and identity theft. Excluding the US, the UK led among the most affected countries followed by Canada, India, Greece and Australia. South Africa is the only other African country among the top 20, ranking sixth with 1,754 complaints." READ MORE

Source: Agence Ecofin

Date: 29 Mar 2021

Le Burkina Faso se dote d'un laboratoire d'investigation numérique pour combattre la cybercriminalité

"En 2020, l'Union européenne et l'Allemagne ont mobilisé 7.5 millions d'euros pour aider les pays d'Afrique de l'Ouest à améliorer leurs réponses aux menaces informatiques. […] Le Burkina Faso se dotera d'un laboratoire d'investigation numérique dont les équipements techniques seront remis, mardi 30 mars à Ouagadougou, par la Commission de la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO), en partenariat avec l'Union européenne (UE) et Expertise France." READ MORE

Source: Brookings

Date: 16 Mar 2021

How African states can improve their cybersecurity

"The COVID-19 pandemic has accelerated digitalization around the world, but as life has shifted increasingly online, cybercriminals have exploited the opportunity to attack vital digital infrastructure. […] In light of increased attacks, institutions such as the Central Bank of Nigeria and national cyber-response organizations in Tunisia, Ivory Coast, Morocco, and Kenya have sounded the alarm to businesses and citizens, urging them to improve security measures. But states across Africa still lack a dedicated public cybersecurity strategy." READ MORE

Source: Digit

Date: 30 Mar 2021

Questions Raised Over Secure Message Evidence in 2020 EncroChat Arrests

"Forensic and legal experts in the UK are questioning the legal 'black hole' of evidence surrounding the EncroChat hack announced in early March. […] The experts claim that evidence presented to courts in the UK would be undermined as French law enforcement officials and prosecutors are refusing to follow typical forensic principles." READ MORE

Source: BBC

Date: 24 Mar 2021

Child abuse: Warning of siblings being groomed online

"Criminals and pedophiles are trying to groom and exploit young siblings as part of an emerging trend of online sexual abuse, experts have warned. The Internet Watch Foundation said victims ranged from 3-16 years, with some groomed to copy adult pornography. It found 511 examples involving siblings between September and December - roughly one in 30 instances of all "self-generated content" in that time. Campaigners say livestreaming services need to do more to protect children. The IWF, which works with police and websites worldwide to take down harmful material, said the Covid-19 pandemic had been a "perfect storm" for the abuse." READ MORE

Source: Cyberscoop

Date: 26 Mar 2021

Hackers target German lawmakers in an election year

"Hackers have attempted to breach the private email accounts of certain German parliamentarians, a spokesperson for the legislative body confirmed Friday […] The attempted intrusions come six months ahead of Germany's national elections. The German parliament has been a recurring target for foreign hackers, including a 2015 breach that the European Union blamed on Russia's military intelligence agency." READ MORE

Source: Sapo

Date: 31 Mar 2021

Portugal alvo de espionagem por parte de outros países

"Portugal foi alvo de ciberataques e espionagem, alguns deles por parte de outros países estrangeiros, com o objetivo de que fossem roubadas informações confidenciais, com valor político e económico, avança o 'Jornal de Notícias' (JN). A informação consta do Relatório Anual de Segurança Interna (RASI) de 2020, a que o jornal teve acesso e que foi aprovado no Conselho Superior de Segurança Interna, na terça-feira, sendo hoje enviado à Assembleia da República." READ MORE

Source: AP News

Date: 17 Mar 2021

Polish state websites hacked and used to spread false info

"Two Polish government websites were hacked Wednesday and used briefly to spread false information about a non-existent radioactive threat, in what a Polish government official said had the hallmarks of a Russian cyberattack. The National Atomic Energy Agency and Health Ministry websites briefly carried claims of a supposed nuclear waste leak coming from neighboring Lithuania and threatening Poland." READ MORE

Source: Hot for Security

Date: 31 Mar 2021

Cyber-attack forces live TV shows off-air on Australia's Channel 9

"Live broadcasts from Australia's Channel 9 TV network were disrupted this weekend following what is believed to have been a cyber-attack. Channel 9 executives later confirmed to The Age that the network had suffered a cyber-attack, and that staff had been ordered to work from home indefinitely while attempts were made to restore systems back to normal operation. Meanwhile, the Australian Parliament in Canberra was said to also be investigating a potential cyber-attack against government-issued smartphones and tablets on Sunday evening." READ MORE

Source: Stuff

Date: 13 Mar 2021

Two years since the March 15 terror attack, the hard work is not over

"Two years after a terrorist killed 51 people and injured dozens at two Christchurch mosques, victims and their families are still struggling with the wide-ranging impacts of the horrific attack. Since March 15, 2019 […] the Ministry for Ethnic Communities is close to being established, police's response to hate crimes strengthened, programmes implemented to prevent terrorist and violent extremism, the Christchurch Call signed by 48 countries, and New Zealand has decided to join the Council of Europe Convention on Cybercrime." READ MORE

Source: The Hacker News

Date: 29 Mar 2021

MobiKwik Suffers Major Breach — KYC Data of 3.5 Million Users Exposed

"Popular Indian mobile payments service MobiKwik on Monday came under fire after 8.2 terabytes (TB) of data belonging to millions of its users began circulating on the dark web in the aftermath of a major data breach that came to light earlier this month. The leaked data includes sensitive personal information such as: customer names, hashed passwords, email addresses, residential addresses, GPS locations, list of installed apps, partially-masked credit card numbers, connected bank accounts and associated account numbers, and know your customer (KYC) documents of 3.5 million users." READ MORE

Source: El Tribuno

Date: 23 Mar 2021

Argentina: Ciberdelitos: crean la Comisión de Reforma del Código Procesal Penal de Salta

"La Comisión de Reforma estará bajo la dirección de la Procuración General y será integrada por el secretario de Justicia, Diego Sebastián Pérez; el director del Instituto de Derecho de las Telecomunicaciones, Informática y Nuevas TICs del Colegio de Abogados y Procuradores, José Aráoz Fleming y representantes de las universidades, bajo la coordinación de la secretaria General de Política Criminal de la Procuración, Sofía Cornejo. […] El procurador general de la Provincia, Abel Cornejo, sostuvo que la aparición de la evidencia digital "implicó un cambio de paradigma en el proceso penal, de tal magnitud que nos llevó a repensar el tratamiento de la prueba en las investigaciones penales y en los códigos de procedimiento." READ MORE

RELATED ARTICLE:

Boletin Oficial Salta, Argentina - RESOLUCIÓN N° 001179, 23 March 2021

Source: Agenda.ge

Date: 18 Mar 2021

Parliament hears bill on stricter punishment for cyber crimes

"The Georgian parliament is hearing a bill by the Ministry of Internal Affairs designed to provide stricter criminal punishment for cybercrimes including hacking for financial gain and creation of fake data. The provision is designed to introduce two new articles into the criminal code. The first of these outlines punishment for acts of hacking into computer systems and/or obtaining data for monetary gain. In comments about the bill the interior ministry said the article was aiming to involve stricter punishment for these acts compared to "other cybercrimes." READ MORE

Source: Council of Europe

Date: 19 Mar 2021

CyberEast: Roundtable discussion on cybercrime and cybersecurity policies and action plans with Moldovan authorities

"The workshop organized under the joint efforts of the CyberEast and Cybersecurity EAST projects funded by the EU facilitated discussion with national counterparts on the progress so far and further plans with regard to cybersecurity and cybercrime policies. The projects in question are ready to support the Moldovan authorities in the implementation process, with specific activities planned together with national counterparts." READ MORE

Source: Security Service of Ukraine

Date: 22 Mar 2021

SBU arrests cyber-fraudsters who extorted from Ukrainians almost USD 5m

"In the city of Kyiv, SBU cyber specialists blocked the activities of an organized group that extorted almost USD 5m from Ukrainians. The offenders misappropriated investors' funds, imitating participation in exchange trading and cryptocurrency transactions. In the network, they simulated electronic trading, and in the "personal accounts" of depositors displayed graphs of value growth of cryptocurrencies and securities. […] During the investigation, law enforcement officers seized incontrovertible evidence of illegal activity. The organizer received a suspicion notice of fraud in especially gross amounts." READ MORE

Source: Council of Europe

Date: 23 Mar 2021

iPROCEEDS-2: Assessment of the investigation and collection/handling of electronic evidence under the domestic legislation

"Under result 4 of the Joint European Union and the Council of Europe iPROCEEDS-2 Project - Capacities of specialized investigative units and inter-agency cooperation further strengthened, an assessment on the investigation and collection/handling of electronic evidence under domestic legislations was conducted in all iPROCEEDS-2 countries/area. The assignment was performed by international experts with extensive practical experience in handling electronic evidence who drafted a comprehensive questionnaire and held online meetings with professional counterparts from all countries/area." READ MORE

Latest reports

- Homeland Security, Joint Statement from the Departments of Justice and Homeland Security Assessing the Impact of Foreign Interference during the 2020 U.S. Elections, 16 March 2021
- FBI, FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, 17 March 2021
- CircleID, The Path to Combatting Domain Abuse, 29 March 2021
- Internet and Jurisdiction Policy Network, Cross-Border Access to Electronic Evidence
- ENISA, When & How to Report Security Incidents, 22 March 2021
- Varonis, Overview: 2021 Cybersecurity Trends to Watch For, 16 March 2021
- Council of Europe, Study on the conformity of personal data provisions with Convention 108+, March 2021
- Communications of the ACM, Cyber Security Research in the Arab Region: A Blooming Ecosystem with Global Ambitions, 22 Mar 2021
- Global Cyber Security Capacity Centre, Cybercrime in ASEAN – Anti-Child Pornography Legislation, 25 Mar 2021
- SSRN, Cybercrime in ASEAN – Anti-Child Pornography Legislation, 25 Mar 2021
- Trilateral Research, Harmonising European cybersecurity strategies to tackle cybercrime, 22 Mar 2021
- ASPI Institute, Counterterrorism Yearbook 2021, 31 March 2021

Upcoming events

- 31 March - 1 April, C-PROC/INTERPOL, (on-line), Workshop on the functioning and role of 24/7 Networks of Contact Points in international cooperation on cybercrime and e-evidence, GLACY+, CyberSouth CyberEast, iPROCEEDS-2
- 31 March - 1 April, C-PROC/MONTENEGRO, (on-line), Business analysis CERT/LEA, iPROCEEDS-2
- 31 March - 1 April, C-PROC/MONTENEGRO, (desk assessment), Guidelines and procedures on sharing of data by CERTs/CSIRTs with criminal justice authorities, iPROCEEDS-2
- 1 - 15 April, C-PROC/Children's Rights Division, (desk assessment), Development and update of Octopus country profiles on OCSEA for Armenia, Azerbaijan, Ukraine, EndOCSEA@Europe, Octopus
- 5 - 8 April, C-PROC/UKRAINE, (on-line), Pilot session of online judicial training, CyberEast
- 7 April, C-PROC, (on-line), African DPA Network Series of regional webinars (sixth workshop), GLACY+
- 7 - 16 April, C-PROC/INTERPOL, (on-line), Series of GLACY+ & INTERPOL webinars on encryption in Spanish, GLACY+
- 8 April, C-PROC/INTERPOL, (on-line), Series of GLACY+ & INTERPOL webinar on darknets and virtual currencies in French, GLACY+
- 9 April, C-PROC, (on-line), 7th C-PROC Anniversary - Capacity building on cybercrime and the COVID-19 pandemic, GLACY+, CyberSouth, CyberEast, EndOCSEA@Europe, iPROCEEDS-2, Octopus
- 12 April, C-PROC/SERBIA, (on-line), Workshop on cybercrime and cybersecurity trends as well as for criminal justice statistics, iPROCEEDS-2
- 12 April, C-PROC/SERBIA, (desk assessment), Reports on cybercrime and cybersecurity trends as well as for criminal justice statistics, iPROCEEDS-2
- 12 April, C-PROC, (online), T-CY, Protocol Drafting Plenary (9), T-CY, Octopus

- 12 April, C-PROC, (online), Working group meeting on the development of an online training platform, Octopus
- 13 - 14 April, C-PROC/SAINT LUCIA, (online), Desk review and Online Workshop on cybercrime legislation and electronic evidence, Octopus project in cooperation with CARICOM IMPACS
- 13 - 15 April, C-PROC/COLOMBIA, (on-line), Online Workshop on Data Protection and INTERPOL tools and services, GLACY+
- 15 April, C-PROC/MONTENEGRO, (on-line), Workshop and hands-on simulation for improvement of the skills, set-up and competencies of 24/7 points of contact, iPROCEEDS-2
- 15 - 16 April, C-PROC/UKRAINE, (on-line), Workshop with personal data protection authorities and national communications regulators on trust and cooperation, CyberEast
- By 15 April, C-PROC, (desk assessment), Development of Guide for first responders to cybercrime investigations, CyberSouth
- By 15 April, C-PROC/Children's Rights Division, Translation, adaption and layout of awareness material 'Kiko and the Manymes' for the project countries, EndOCSEA@Europe
- By 15 April, C-PROC, (desk assessment), Development of standard training on templates for data preservation and subscriber information, 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 March 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