Cybercrime Digest

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

16 – 31 January 2022

Source: Council of Europe

Date: 02 Feb 2022

The global state of cybercrime legislation: Update as at 31 January 2022!

"Countries around the world keep making progress in the strengthening of their criminal laws on cybercrime. […] Today, 128 UN Member States (66%) are considered to have criminalized offences against and by means of computers largely in line with the Budapest Convention on Cybercrime. This represents a considerable increase in the two years since the last survey, in particular in the African region, and recently also in the Pacific. An increase is also noted with respect to procedural powers to secure electronic evidence: 93 States (48%) now have provisions in place corresponding to Articles 16 to 21 of the Budapest Convention." READ MORE

RELATED REPORT:

Council of Europe, Global State of Cybercrime Legislation 2013-2022: A Cursory Overview, 2 February 2022

Source: Council of Europe

Date: 25 Jan 2022

GLACY+: Reviewing project progress and planning activities for 2022 during the 11th Steering Committee meeting

"During the meeting, the project team, GLACY+ priority and hub countries and project partners actively engaged in a review of the key activities delivered in the second half of 2021, including support to strengthen national legislation, strategies and policies on cybercrime and electronic evidence in line with international standards, and to reinforce the capacities of law enforcement and criminal justice authorities to investigate and prosecute cybercrimes." READ MORE

Source: Europol

Date: 21 Jan 2022

Unhappy New Year for cybercriminals as VPNLab.net goes offline

"On 17 January, disruptive actions took place in a coordinated manner in Germany, the Netherlands, Canada, the Czech Republic, France, Hungary, Latvia, Ukraine, the United States and the United Kingdom. Law enforcement authorities have now seized or disrupted the 15 servers that hosted VPNLab.net's service, rendering it no longer available. Led by the Central Criminal Office of the Hannover Police Department in Germany, the action took place under the EMPACT security framework objective Cybercrime - Attacks Against Information Systems." READ MORE

Source: People Matters

Date: Jan 2022

WEF Davos Agenda 2022: Cybercrime spikes at record-breaking speed

"Ransomware threats top the list of cyber-attacks organizations are most concerned about, followed by malicious insider activities and social-engineering attacks, finds the World Economic Forum's Global Cybersecurity Outlook 2022, launched at their annual Davos summit." READ MORE

Source: ICRC

Date: 19 Jan 2022

Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people

"A sophisticated cyber security attack against computer servers hosting information held by the International Committee of the Red Cross (ICRC) was detected this week. The attack compromised personal data and confidential information on more than 515,000 highly vulnerable people, including those separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention. The data originated from at least 60 Red Cross and Red Crescent National Societies around the world." READ MORE

Source: Interpol

Date: 19 Jan 2022

Nigerian cybercrime fraud: 11 suspects arrested, syndicate busted

"The Nigerian Police Force (NPF) has arrested 11 alleged members of a prolific cybercrime network as part of a national police operation coordinated with INTERPOL. Arrested by officers of the NPF Cybercrime Police Unit and INTERPOL's National Central Bureau (NCB) in Nigeria, many of the suspects are thought to be members of 'SilverTerrier', a network known for Business Email Compromise (BEC) scams which have harmed thousands of companies globally." READ MORE

Source: Europol

Date: 26 Jan 2022

Cryptocurrencies: tracing the evolution of criminal finances

"Cryptocurrencies are a technical and financial innovation that offer major potential for the global economy. At the same time, they are being used for criminal purposes such as money laundering, fraud, and the online trade of illicit goods and services. The ways criminals use cryptocurrencies is evolving, and it is spreading to all forms of serious and organised crime." READ MORE

RELATED REPORT:

Europol, Europol Spotlight - Cryptocurrencies - Tracing the evolution of criminal finances, 26 January 2022

Source: Eurojust

Date: 27 Jan 2022

Bulgarian authorities take down online investment scam responsible for losses of more than EUR 10 million

"Judicial and law enforcement authorities in Bulgaria, supported by Europol and Eurojust, have taken down a network of online investment fraudsters involved in money laundering. On the action day on 26 January, officers from the Bulgarian National Police arrested one suspect for defrauding mainly German and Greek investors of at least EUR 10 million. During the action day, a total of 24 locations were searched, while officers interrogated 66 witnesses in Sofia and Burgas. Furthermore, a variety of electronic equipment, financial information and recordings were seized." READ MORE

RELATED ARTICLE:

Europol, Bulgarian authorities take down online investment scam responsible for losses of more than EUR 10 million, updated 1 February 2022

Source: EDPS

Date: 21 Jan 2022

International cooperation to fight crime should comply with EU law

"The EDPS published on 20 January 2022 his Opinion on two Proposals: one to authorise EU Member States to sign the second Protocol to the Budapest Convention on Cybercrime, and one to authorise EU Member States to ratify this same Protocol." READ MORE

RELATED ARTICLE:

European Data Protection Supervisor, EDPS Opinion on the two Proposals for Council Decisions authorising Member States to sign and to ratify in the interest of the EU the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, 20 January 2022

Source: European Commission

Date: 30 Jan 2022

Regulation is needed in the fight against Child Sexual Abuse (CSA) online – companies must use their technical capacity

"Ylva Johansson: "I met with the 'big players', like Apple, Google, Meta and Microsoft and medium size companies like Snap and Roblox. […] After discussions here, I am more convinced than ever that EU legislation is urgently needed to detect and report CSA online and remove CSAM. Detection can literally save a child's life. The legislation will have to reflect the different technical challenges, but it must not be 'time-capsuled' by them. What I mean by that is that we need to set parameters that anticipate the world of 2030 and beyond with a technology-neutral and future-proof legislation. […]"" READ MORE

Source: Reuters

Date: 25 Jan 2022

Twitter sees record number of govt demands to remove content

"Twitter said this was the largest number of accounts ever targeted with government removal requests in a reporting period since the company started releasing transparency reports in 2012. It was also the largest number of government removal requests in a reporting period. […] The number of accounts specified in the legal requests was up almost 50% from 131,933 accounts from the previous six months, according to the data. The number of government removal requests increased 14% from 38,524 in the last reporting period and was up about 2.8% year-over-year, Twitter said." READ MORE

Source: ENISA

Date: 27 Jan 2022

Beware of Digital ID attacks: your face can be spoofed!

"The report on remote identity proofing builds on the previous report Remote ID Proofing of ENISA, which makes an analysis of the different methods used to carry out identity proofing remotely. The new report analyses the different types of face recognition attacks and suggests countermeasures. It also validates the security controls introduced in the previous report and offers further recommendations on how to mitigate identified threats." READ MORE

Source: Security Week

Date: 24 Jan 2022

Russian Authorities Arrest Head of International Cybercrime Group

"Last week, Russian authorities – Moscow's FSB security agency included – arrested Andrey Sergeevich Novak, an alleged co-founded and leader of the organization. In 2018, the DoJ indicted Novak for his role in the group's transnational racketeering conspiracy and on three other counts." READ MORE

Source: The Clinic

Date: 26 Jan 2022

Chile: Rechazo en bloque genera ley sobre entrega de datos personales a Fiscalía sin orden judicial

"Un transversal rechazo ha generado una ley tendiente a facultar al Ministerio Público a solicitar datos personales sin orden judicial. Esta vez, la industria, académicos y activistas criticaron la modificación al Código Procesal Penal aprobada por una comisión mixta en el Congreso. Se trata de una actualización de la ley de Delitos Informáticos que pondría a Chile a la par del Convenio de Budapest, según informó Diario Financiero. La normativa data de 1993 y también "busca poner al día algunas materias para perseguir" este tipo de infracciones." READ MORE

RELATED ARTICLE

El Mostrador, Proyecto que entrega datos personales a Fiscalía sin orden judicial para investigar delitos informáticos genera polémica sobre la vigilancia en el ciberespacio, 28 January 2022

Source: AP News

Date: 22 Jan 2022

Bitcoin pyramid schemes wreak havoc on Brazil's 'New Egypt'

"Police say the company owned by 38-year-old Glaidson Acácio dos Santos had total transactions worth at least $7 billion ($38 billion reais) from 2015 through mid-2021 as part of a Bitcoin-based Ponzi scheme that promised investors 10% monthly returns. In hundreds of pages of documents obtained by The Associated Press, federal and state police and prosecutors accuse dos Santos and his associates of running a sophisticated racket defrauding thousands of small-scale investors who believed they were getting rich off Bitcoin's steep appreciation." READ MORE

Source: News Ghana

Date: 18 Jan 2022

12 Countries across Sub-Saharan Africa gathers together in Ghana to address cybercrime

"The conference has drawn experts from across Sub-Saharan Africa, including investigators, prosecutors and senior judiciary, as well as Attorneys General and Authorities engaged in combating cybercrime, to enhance cyber-capability and resilience of regional authorities in western Africa in support of the Commonwealth Heads of Government's Cyber Declaration, in London 2018. […] "Dr. Albert Antwi-Boasiako said "The Government of Ghana, working closely with the Council of Europe through the GLACY+ Project has trained more than three thousand five hundred (3,500) criminal justice officials, including Judges, Prosecutors and Investigators on cybercrime and electronic evidence in the last five years and this has significantly improved criminal justice response to cybercrimes.[…]"" READ MORE

Source: Opera News

Date: 20 Jan 2022

Microsoft and Attorney General Alliance partner to build cybersecurity capacity in Africa

"Microsoft and The Attorney General Alliance (AGA) an organisation committed to building capacity and exchanging knowledge with African governments, justice and law enforcement agencies and officials throughout Africa to support the rule of law and combat transnational criminal activity have today launched a partnership today. The two organisations will collaborate with government, justice and law enforcement agencies and officials across Africa to train and share knowledge and experience with the aim of capacity building focusing on cybercrime and other related cross-border criminal activity like money laundering." READ MORE

Source: Reuters

Date: 30 Jan 2022

Crypto giant Binance restricts 281 Nigerian accounts

"Binance, the world's largest cryptocurrency exchange, has restricted the personal accounts of 281 Nigerian users, citing a need to comply with international money laundering laws, its CEO said. Changpeng Zhao said in a letter to Nigerian customers dated Jan. 29 that the decision to restrict some personal accounts was to ensure user safety while more than a third of the affected accounts were restricted at the request of international law enforcement." READ MORE

Source: Middle East Monitor

Date: 17 Jan 2022

Morocco introduces new cybercrime laws

"The Moroccan Minister of Justice, Abdellatif Wehbe, said the Ministry is working to introduce new legal requirements aimed at combating cyber crimes, especially those targeting women and children. He explained that, in the context of ensuring compatibility with international standards, especially the Budapest Convention on cybercrime, the Ministry of Justice, as part of its comprehensive review of the Criminal Law and Criminal Procedure Group, has included a set of important developments, especially related to the rules of research and investigation of cybercrime." READ MORE

Source: LiveLaw.in

Date: 29 Jan 2022

India: Prosecution has right to ask accused to surrender mobile phone

"The Kerala High Court on Saturday held that the prosecution has every right to seek that the accused should surrender mobile phones for forensic examination under Section 79A of the Information Technology Act. The Court rejected the argument that the surrender of mobile phones will infringe the fundamental right against self-incrimination under Article 20(3) of the Constitution of India." READ MORE

Source: The Diplomat

Date: 31 Jan 2022

Myanmar Junta Set to Pass Draconian Cyber Security Law

"Myanmar's military junta is reportedly on the brink of passing its long-threatened cybersecurity law, which in its latest form would outlaw virtual private networks (VPNs), throttle access to social media networks, and force internet companies to hand over user data to the military. " READ MORE

Source: Reuters

Date: 26 Jan 2022

N. Korean internet downed by suspected cyber-attacks - researchers

"North Korea's internet appears to have been hit by a second wave of outages in as many weeks, possibly caused by a distributed denial-of-service (DDoS) attack, researchers said on Wednesday. The latest incident took place for about six hours on Wednesday morning local time and came a day after North Korea conducted its fifth missile test this month." READ MORE

Source: ZDNet

Date: 20 Jan 2022

Singapore police warns of ad scams targeting Google search users

"Singapore Police Force (SPF) said these phishing ads would pop up on Google when users searched for a bank's contact number with the intention of seeking advice for various reasons. These ads would show up amongst the first few search results and contain fake contact details for the bank, the police said in its advisory note released Wednesday." READ MORE

Source: OSCE

Date: 26 Jan 2022

CyberEast Project and OSCE: training course on financial investigations, virtual currencies and darknet in Armenia

"OSCE, jointly with the Council of Europe, organized a training course on financial investigations, cryptocurrencies and the use of the darknet for police officers, prosecutors, and representatives of the National Security Service, Investigative Committee, and the Central Bank of Armenia. Over 20 participants attended the training course held from 19 to 21 January in Yerevan." READ MORE

Source: CNN

Date: 25 Jan 2022

Hackers target Canada's foreign ministry in cyber attack

"Canadian cybersecurity officials were working to restore those internet services as of Monday night. "Critical services for Canadians" through the foreign ministry were not affected by the incident, the Treasury Board of Canada Secretariat, a government agency, said in a statement to CNN. "At this time, there is no indication that any other government departments have been impacted by this incident," the statement said." READ MORE

Source: Threat Post

Date: 19 Jan 2022

Cloned Dept. of Labor Site Hawks Fake Government Contracts

"A well-crafted but fake government procurement portal offers the opportunity to submit a bid for lucrative government projects — but harvests credentials instead. A new phishing campaign is targeting aspiring government vendors with an invitation to bid on various fake federal projects with the U.S. Department of Labor. Emails branded to look like legitimate communications from the DoL contain malicious links that, rather than leading to a government procurement portal, harvest the credentials of anyone who attempts to login, according to a new report from threat researchers at INKY." READ MORE

Source: Government of Canada

Date: 26 Jan 2022

Canada: CRTC investigation targets Dark Web marketplace vendors and administrator

"The CRTC's Chief Compliance and Enforcement Officer today announced penalties totalling $300,000 to four Canadians for their involvement in the Dark Web marketplace Canadian HeadQuarters (also known as CanadianHQ). The marketplace was taken offline following the execution of warrants by CRTC staff. Before shutting down, CanadianHQ was one of the largest Dark Web marketplaces in the world and significantly contributed to harmful cyber activity in Canada. It specialized in the sale of goods and services, including spamming services, phishing kits, stolen credentials and access to compromised computers, which were used by purchasers to engage in a variety of malicious activities." READ MORE

Source: NCA

Date: 17 Jan 2022

Rise in school cybercrime attacks sparks NCA education drive

"A new initiative to divert young people away from criminality has been launched after cyber-attacks designed to block access to schools' networks or websites more than doubled during the Covid-19 pandemic. Data from the National Crime Agency's National Cyber Crime Unit (NCCU) shows there was a 107 per cent increase in reports from the police cyber prevent network of students as young as nine deploying DDoS (distributed denial of service) attacks from 2019 to 2020. Many referrals into the NCCU's Prevent team are for children of secondary school age, with the median age at 15 and the youngest at nine." READ MORE

Source: DW

Date: 29 Jan 2022

Pegasus scandal: In Hungary, journalists sue state over spyware

"The Pegasus scandal became more widely known in July 2021, when a journalism network published information about leaked lists of around 50,000 phone numbers that had been targeted and attacked using the Israeli spyware. Some 300 of the targets were based in Hungary, and they included the phones of journalists, lawyers, political activists, entrepreneurs — even a former minister." READ MORE

Source: The Brussels Times

Date: 27 Jan 2022

Belgium to spend millions improving national cyber security

"Dermine detailed the cyber investments while speaking at the 14th European Space Conference, held Tuesday and Wednesday at the Egmont Palace in Brussels. The recovery plan involves 105 investments and 35 reforms designed to prepare Belgium for ongoing digital and environmental changes. According to the European Commission, more than a quarter of the €5.9 billion plan is supporting digital upgrades." READ MORE

Latest reports

- Atlas VPN, 50 Worrying Cybercrime Statistics & Facts [2022], 17 January 2022
- CyberSixGill, Telegram: A Cybercriminal Hotspot – Compromised Financial Accounts, 17 January 2022
- World Economic Forum, Global Cybersecurity Outlook 2022, 18 January 2022
- Federal Bureau of Investigations, Indicators of compromise associated with Diavol Ransomware, 19 January 2022
- Barracuda, Threat Spotlight: COVID-19 test-related email scams, 20 January 2022
- HelpNet Security, Cyber risks top worldwide business concerns in 2022, 20 January 2022
- Security Week, Security Scanners Across Europe Tied to China Govt, Military, 20 January 2022
- ENISA, Remote Identity Proofing - Attacks & Countermeasures, 20 January 2022
- Proof Point, Threats Are (Still) on the Rise: 2022 Ponemon Report, 25 January 2022
- Eurnews Travel, How will contactless tech transform travel in 2022?, 25 January 2022
- CTED, The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives, 25 January 2022
- Threatpost, 'Dark Herring' Billing Malware Swims onto 105M Android Devices, 26 January 2022
- Europol, Cryptocurrencies: tracing the evolution of criminal finances, 26 January 2022
- Malwarebytes, Cyberinsurance companies don't want to pay out for "acts of war", 26 January 2022
- ENISA, Data Protection Engineering, 27 January 2022
- European Parliament: Cybersecurity: main and emerging threats in 2021 (infographic), 27 January 2022
- Tech Against Terrorism, Report: The Threat of Terrorist and Violent Extremist Operated Websites, 28 January 2022
- Police1.com: 16 features to look for in a Digital Evidence Management System (DEMS), 28 January 2022
- Embroker, 2022 Must-Know Cyber Attack Statistics and Trends, 31 January 2022
- WeLiveSecurity, How to tell if your phone has been hacked, 31 January 2022
- Chatam House, Europe regional consultation: strengthening effective and inclusive cybercrime policymaking, January 2022
- Biblioteca del Congreso Nacional de Chile/ BCN, Ciberseguridad e inteligencia artificial en Chile, January 2022
- KPMG, Una triple amenaza en las Américas, Fraud survey report, spanish version, January 2022
- Forbes.com: Predicting What 2022 Holds For Cybersecurity, January 2022

Upcoming events

- 1 February, C-PROC/JORDAN, (*online*), Third Working Group Meeting on the mainstreaming of judicial training material on cybercrime and electronic evidence, CyberSouth
- 1-15 February, C-PROC/ PHILIPPINES, (*desk study*), Study on the COVID-19 related cybercrime and e-evidence, OCTOPUS
- 2 February, C-PROC/PHILIPPINES, (*online*), Kick off meeting of the assessment of the COVID-19 related cybercrime and e-evidence, OCTOPUS
- 2-4 February, C-PROC/GEORGIA, (*in-person*), Training on interagency cooperation and financial investigations/intelligence, CyberEast
- 7-9 February, C-PROC/AZERBAIJAN, (*online*), Law enforcement training for investigators and prosecutors with MIA Academy and MoJ Academy, CyberEast
- 8 February, C-PROC, (*online*), Series of roundtables on the Second Additional Protocol for LATAM and Caribbean countries, GLACY+, OCTOPUS
- 8 February, C-PROC/LEBANON, (*online*), National Workshop on the preparation of criminal justice statistics on cybercrime and e-evidence, CyberSouth
- 8-11 February, C-PROC/ KOSOVO*, (*online*), Training skill certification programme for judges and prosecutors delivering Council of Europe judicial training on cybercrime and electronic evidence, iPROCEEDS-2
- 9-11 February, FRANCE, INTERPOL, International Database on the Sexual Exploitation of Children (ICSE), iPROCEEDS-2
- 14-18 February, C-PROC/DOMINICAN REPUBLIC/COLOMBIA, ECTEG eFIRST meeting, GLACY+
- 15 February, C-PROC, (*online*), Series of webinars on the Second Additional Protocol: JITs & joint investigations, GLACY+, OCTOPUS
- 15 February, C-PROC/TUNISIA, (*online*), National Workshop on the preparation of criminal justice statistics on cybercrime and e-evidence, CyberSouth

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 February have been rescheduled to a later date.

The Cybercrime Digest appears bi-weekly. The news is selected by relevance to the current areas of interest to C-PROC and does 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