Cybercrime Digest

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

16 – 30 September 2021

Source: Council of Europe

Date: 28 Sep 2021

20 years of the Convention on Cybercrime: join the celebration!

"In November 2001, the Convention on Cybercrime was opened for signature in Budapest, Hungary. Twenty years on, that treaty, known as the "Budapest Convention", remains the most relevant international agreement on cybercrime and electronic evidence. Join us on our 20th anniversary website to find out more about the Convention! From 16 to 18 November, we will hold the Octopus Conference 2021. A special event with high level interventions will take place on 16 November in cooperation with the Hungarian Chairmanship of the Committee of Ministers on the occasion of this 20th anniversary of the Convention as well as the forthcoming 2nd additional Protocol on enhanced cooperation and disclosure of electronic evidence."

Source: Council of Europe

Date: 21 Sep 2021

Japan makes a voluntary contribution

"The Government of Japan has made a voluntary contribution of €45,000 to support the prevention of violence against women and the Council of Europe action against cybercrime. The agreement was signed on 21 September 2021 by Ambassador Takeshi Akamatsu, Permanent Observer of Japan to the Council of Europe, and Mr Bjørn Berge, Deputy Secretary General." READ MORE

Source: Eurojust

Date: 17 Sep 2021

CrimEx experts start work on development of six cooperation tools

"The CrimEx expert group in criminal matters has decided to set up a series of six key tools for judicial and law enforcement cooperation with the South Partner Countries participating in the EuroMed Justice (EMJ) programme. These tools will now be further developed by high-level Short-Term Experts (STEs) who have been engaged to support the CrimEx group. They will enable asset recovery, protection of personal data, joint and parallel investigations, procedural rights of defendants and victims, bilateral agreements and the transfer of electronic evidence across the Mediterranean." READ MORE

Source: EURACTIV

Date: 16 Sep 2021

EU chief announces cybersecurity law for connected devices

"European Commission President Ursula von der Leyen announced on Wednesday (15 September) a Cyber Resilience Act aimed at setting common cybersecurity standards for connected devices. […] The Commission initiative adds to an existing proposal for a Directive on Security of Network and Information Systems, commonly known as the NIS2 Directive. [...] The internet of things will bring about a great deal of unsecured products, because security is often not on top of the mind of the producers of such machines. And there is no European standard yet to be upheld. It's nice to have a pulled pork machine in your kitchen, or a smart coffee machine, but it is also a way hackers can enter your home IT systems," Groothuis told EURACTIV." READ MORE

Source: The Hacker News

Date: 24 Sep 2021

US Sanctions Cryptocurrency Exchange SUEX for Aiding Ransomware Gangs

"The U.S. Treasury Department on Tuesday imposed sanctions on Russian cryptocurrency exchange Suex for helping facilitate and launder transactions from at least eight ransomware variants as part of the government's efforts to crack down on a surge in ransomware incidents and make it difficult for bad actors to profit from such attacks using digital currencies. […] "SUEX is being designated pursuant to Executive Order 13694, as amended, for providing material support to the threat posed by criminal ransomware actors."" READ MORE

RELATED ARTICLE:

US Treasury, Treasury Takes Robust Actions to Counter Ransomware, 21 Sep 2021

Source: Europol

Date: 20 Sep 2021

106 arrested in a sting against online fraudsters

"The Spanish National Police (Policía Nacional), supported by the Italian National Police (Polizia di Stato), Europol and Eurojust, dismantled an organised crime group linked to the Italian Mafia involved in online fraud, money laundering, drug trafficking and property crime. The suspects defrauded hundreds of victims through phishing attacks and other types of online fraud such as SIM swapping and business email compromise before laundering the money through a wide network of money mules and shell companies. Last year alone, the illegal profit is estimated at about € 10 million.'' READ MORE

RELATED ARTICLE:

Vice, How the Mafia Is Pivoting to Cybercrime, 22 September 2021

Source: Council of Europe

Date: 22 Sept 2021

Civil society, new technologies and rights

"On September 21, Patrick Penninckx, Head of the Information Society Department addressed the participants of the Recharging advocacy for Rights in Europe (RARE) programme in Amsterdam. [...] The presentation "New technologies and rights: the Council of Europe approach" outlined the latest technological developments and their impact on human rights, and emphasised the Council of Europe's responses on the policy and implementation levels in the areas of freedom of expression, media freedom, privacy, internet governance, cybercrime and artificial intelligence. The speaker further underlined the important role civil society organisations, NGOs and human rights defenders play as both partners and beneficiaries of the Council of Europe, the current areas and tools of cooperation as well as new opportunities to explore.'' READ MORE

Source: Irish Examiner

Date: 15 Sep 2021

Irishman and 'world's biggest facilitator' of child sex abuse images to be sentenced

"Eric Eoin Marques, who has been described as the world's biggest facilitator for child sexual abuse imagery, is due to be sentenced by a US court later today. […]Marques pleaded guilty in February 2020, as part of a plea agreement, admitting that between July 24, 2008, and July 29, 2013, he conspired to advertise child sexual abuse by operating an anonymous hosting service on the dark web. […]Investigators found what appeared to be more than 8.5m images and videos of child abuse on the Freedom Hosting server, according to a court filing that accompanied Marques' guilty plea." READ MORE

Source: Council of the EU

Date: 24 Sep 2021

Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes

"Some EU Member States have observed malicious cyber activities, collectively designated as Ghostwriter, and associated these with the Russian state. […] These malicious cyber activities are targeting numerous members of Parliaments, government officials, politicians, and members of the press and civil society in the EU by accessing computer systems and personal accounts and stealing data. These activities are contrary to the norms of responsible State behaviour in cyberspace as endorsed by all UN Member States, and attempt […] The European Union and its Member States strongly denounce these malicious cyber activities, which all involved must put to an end immediately." READ MORE

Source: Phys.org

Date: 17 Sep 2021

Digital evidence at risk of being missed because of fragmented police training and coordination, study warns

"There is a risk of crucial digital evidence being missed or misinterpreted because of a shortage of adequate skills and knowledge in police forces, a new study warns. The findings highlight the need for the on-going training for police officers who routinely draw upon digital evidence in their investigations. […] Experts also found increased demand in the processing of digital evidence and the isolation of digital forensic units from operational policing units can lead to few opportunities for sustained collaboration or sharing of expertise between officers and digital forensic practitioners." READ MORE

Source: The Threat Post

Date: 15 Sep 2021

Attackers Impersonate DoT in Two-Day Phishing Scam

"Threat actors impersonated the U.S. Department of Transportation (USDOT) in a two-day phishing campaign that used a combination of tactics – including creating new domains that mimic federal sites so as to appear to be legitimate – to evade security detections. […] The campaign – which targeted companies in industries such as engineering, energy and architecture that likely would work with the USDOT – sends potential victims an initial email in which they're told that the USDOT is inviting them to submit a bid for a department project by clicking a big blue button with the words "Click Here to Bid."" READ MORE

Source: B&FT Online

Date: 01 Oct 2021

Meet Dr. Antwi-Boasiako; first ever Director-General of Ghana's Cyber Security Authority

"President Nana Addo Dankwa Akufo-Addo has appointed Dr Albert Antwi-Boasiako as the Acting Director-General of the Cyber Security Authority (CSA) effective October 1, 2021. Prior to this appointment, he served as the National Cybersecurity Advisor and Head of the National Cyber Security Centre (NCSC), , leading Ghana's institutionalisation of cybersecurity under the policy direction of the Minister for Communications & Digitalisation, Hon Ursula Owusu-Ekuful, who is responsible for cybersecurity matters in government." READ MORE

Source: Bleeping Computer

Date: 15 Sep 2021

Ransomware encrypts South Africa's entire Dept of Justice network

"The justice ministry of the South African government is working on restoring its operations after a recent ransomware attack encrypted all its systems, making all electronic services unavailable both internally and to the public. […] "[The attack] has led to all information systems being encrypted and unavailable to both internal employees as well as members of the public. As a result, all electronic services provided by the department are affected, including the issuing of letters of authority, bail services, e-mail and the departmental website" - Steve Mahlangu, spokesperson for the Department of Justice and Constitutional Development" READ MORE

Source: Council of Europe

Date: 20 Sep 2021

GLACY+: Workshop on cybercrime, electronic evidence legislation and fundamental rights in Burkina Faso

"In cooperation with the Burkinabe authorities and OCWAR-C project and with the support of UNODC and UNOCT, the GLACY+ Project organized a hybrid workshop on Burkina Faso's laws on cybercrime and electronic evidence. Participants from national institutions involved in Burkina Faso's legislative reforms and their enforcement, were actively engaged in discussions on various topics. The dialogue focused on substantive provisions, procedural powers, interagency cooperation, the link between cybercrime and terrorism as well as on best practices to efficiently counteract these threats." READ MORE

Source: Council of Europe

Date: 16 Sep 2021

CyberSouth: Mainstreaming of cybercrime judicial training. Third meeting of the working group in Algeria

"Under the CyberSouth project, the third meeting for mainstreaming the judicial training in Algeria took place online, on the 16th of September 2021. This event was a follow-up to the second meeting of the working group focused on developing the Algerian course on cybercrime and electronic evidence for magistrates." READ MORE

Source: OpenGov Asia

Date: 08 Sep 2021

Philippine Banks Urged Deployment of Anti-Cybercrime Law for Consumers

"[…] The Bangko Sentral ng Pilipinas (BSP) has once again urged the immediate establishment of an anti-cybercrime law to better protect financial consumers. According to the BSP, Senate Bill No. 2380, also known as the "Bank Account, E-wallet, and Other Financial Accounts Regulation Act," is a bill that recognises the need to protect the public from cybercriminals and syndicates who target bank accounts and e-wallets.[...] If the bill is passed, agencies such as the Bank of the Philippines, the Department of Justice, the Department of Information and Communications Technology, the National Bureau of Investigation, and the Philippine National Police will create an "Anti-Scam/Financial Fraud Roadmap" to educate and inform consumers about financial scams and how to avoid them, as well as to expedite regulation." READ MORE

Source: Securoity Affairs

Date: 21 Sep 2021

Data of 106 million visitors to Thailand leaked online

"The popular cybersecurity research Bob Diachenko discovered his personal data online stored on an unprotected Elasticsearch database containing the personal details of more than 106 million visitors to Thailand. The expert discovered the unsecured database on August 22, 2021, and immediately notified the Thai authorities, he noticed that some of the data stored in the archive date back ten years. Exposed records include full names, arrival dates, gender, residency status, passport numbers, visa information, and Thai arrival card numbers." READ MORE

Source: Telecom.com

Date: 14 Sep 2021

Japan mulls tougher punishment for cyber crime

"Japanese Justice Minister Yoko Kamikawa said on Tuesday that the country is considering the introduction of a tougher jail sentence as part of penalties for cybercrimes. […] With the legislation, which is expected to be effective in the fall of next year, victims can obtain information of the harassers through only one court proceeding instead of going through at least two court proceedings, with one of them for social media operators and the other for the internet service provider, at present.." READ MORE

Source: La Jornada

Date: 15 Sep 2021

Urgen a que México firme el Convenio de Budapest

"El Senado exhortó al gobierno federal a concluir la etapa de evaluación del marco jurídico vigente para que México se adhiera a la Convención sobre Ciberdelincuencia o Convenio de Budapest, ya que tiene "más de 10 años analizándolo para proceder a su ratificación. […] La senadora del PVEM Alejandra Lagunes resaltó que al concretar su adhesión al Convenio de Budapest, México estaría fortaleciendo las acciones nacionales en materia de ciberseguridad y colaborando con otros países en la lucha efectiva contra la ciberdelincuencia." READ MORE

Source: the Hacker News

Date: 20 Sep 2021

A New Wave of Malware Attack Targeting Organizations in South America

"A spam campaign delivering spear-phishing emails aimed at South American organizations has retooled its techniques to include a wide range of commodity remote access trojans (RATs) and geolocation filtering to avoid detection, according to new research. […]Multiple verticals, including government, financial, healthcare, telecommunications, and energy, oil, and gas, are said to have been affected, with a majority of the targets for the latest campaign located in Colombia and a smaller fraction also coming from Ecuador, Spain, and Panama.." READ MORE

Source: Senado Republica de Chile

Date: 29 Sep 2021

Chile: A Comisión Mixta proyecto que tipifica los delitos informáticos

"La Sala podría abocarse a revisar el informe que emitirá la Comisión de Seguridad Pública respecto del proyecto que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest**.** Esto luego que sus integrantes rechazaran parte de los cambios realizados al texto por los diputados y diputadas. De hecho, los legisladores recomendarán la conformación de una Comisión Mixta para buscar una redacción consensuada." READ MORE

Source: Council of Europe

Date: Jan – Sep 2021

CyberEast: Working together with Azerbaijan on country's first dedicated Cybersecurity/Cybercrime Strategy

"[…] Countries of the Eastern Partnership have committed to implement the Budapest Convention on Cybercrime as a framework for domestic measures and for international cooperation on cybercrime and access to electronic evidence. Furthermore, the EaP countries adopted in October 2013 (Kyiv, Ukraine) a Declaration on Strategic Priorities for the Cooperation against Cybercrime in the EaP Region. As part of event series addressing the policy matters of cybercrime and cybersecurity, a one-day online roundtable was organized with authorities of Azerbaijan on the draft Strategy and Action Plan on Cybersecurity currently in development." READ MORE

Source: Cyjax

Date: 16 Sep 2021

EMEA and APAC governments targeted in widespread credential harvesting campaign

"Cyjax analysts have uncovered a large credential harvesting campaign targeting multiple government departments in APAC and EMEA countries. Over 50 hostnames were analysed, many of which were posing as the Ministry of Foreign Affairs, Ministry of Finance, or Ministry of Energy, in various countries such as Uzbekistan, Belarus, and Turkey; as well as the Main Intelligence Directorate of Ukraine and the Pakistan Navy. It is currently unknown how the attackers are spreading the credential harvesting pages, as no phishing emails have yet been uncovered. Phishing links are, however, the most likely method of distribution." READ MORE

Source: Council of Europe

Date: Jul – Sep 2021

iPROCEEDS-2: Simulation Exercise on Joint Action against Cybercrime

"The iPROCEEDS-2 project aims to support the project countries/area in building and maintaining partnerships with private sector entities, primarily ISPs, for reinforcing mechanisms for trusted cooperation between the private sector, citizens, and criminal justice authorities. To this end, from July to September, the project delivered a practical exercise scenario that looked to test the cooperation between the ISPs, law enforcement, judicial and cybersecurity authorities in Serbia, Turkey, Kosovo*[1] and Bosnia and Herzegovina." READ MORE

Source: The Straits Times

Date: 16 Sep 2021

Mass personal data theft from Paris Covid-19 tests, say hospitals

"Hackers stole the personal data of around 1.4 million people who took Covid-19 tests in the Paris region in the middle of 2020, hospital officials in the French capital disclosed on Wednesday (Sept 15). Hospital officials said they filed a complaint with the Paris prosecutor's office on Wednesday after confirming on Sept 12 that such a cyber attack took place over the summer. Stolen were the identities, social security numbers and contact details of people tested as well as the identities and contact details of health professionals who dealt with them, along with the test results, the hospital organisation said." READ MORE

Source: Bitcoin.com

Date: 21 Sep 2021

Poland Confirms Arrest of Former Wex Exchange Executive in Warsaw

"Reports of the detention of Dmitry Vasiliev, ex-head of the bankrupt cryptocurrency exchange Wex, have been confirmed by authorities in Poland. The former executive of the platform, allegedly involved in the theft of funds worth millions of dollars, faces possible extradition to Kazakhstan. […] Polish police detained the former Wex CEO with help from Interpol, the International Criminal Police Organization. […] Dmitry Vasiliev is suspected of involvement in the disappearance of $450 million worth of assets belonging to citizens of EU member states and other countries around the world." READ MORE

Source: The Record

Date: 24 Sep 2021

Major European call center provider goes down in ransomware attack

"GSS, the Spanish and Latin America division of Covisian, one of Europe's largest customer care and call center providers, has suffered a debilitating ransomware attack that froze a large part of its IT systems and crippled call centers across its Spanish-speaking customerbase. Among the affected services are Vodafone Spain, the MasMovil ISP, Madrid's water supply company, television stations, and many private businesses, a source familiar with the attack told The Record." READ MORE

Latest reports

- Censinet, Ponemon Research Report: The Impact of Ransomware on Healthcare During COVID-19 and Beyond, September 2021
- European Securities and Markets Authority, ESMA Report on Trends, Risks and Vulnerabilities, 1 September 2021
- Threat Post, Financial Cybercrime: Why Cryptocurrency is the Perfect 'Getaway Car', 9 September 2021
- Trend Micro, Attacks from all angles: 2021 Midyear Cybersecurity Report, 14 September 2021
- Euler Hermes France, 1 entreprise sur 4 a subi une fraude avérée cette année, 15 September 2021
- Australian Cybersecurity Centre, ACSC Annual Cyber Threat Report 2020-21, 15 September 2021
- Security Report, A evolução dos ataques cibernéticos: Até onde os hackers podem ir?, 16 September 2021
- Humanitarian Law & Policy, Signalling legal protection in a digitalizing world: a new era for the distinctive emblems?, 16 September 2021
- Security Intelligence, How to Protect Against Deepfake Attacks and Extortion, 17 September 2021
- Les Numeriques, La cybercriminalité, un "Far West numérique" au cœur des relations internationales, 20 September 2021
- The State of Security, How to Report a Data Breach per GDPR, 20 September 2021
- Business Wire, Threat Intelligence Report de NETSCOUT H1 2021 : les cyberattaques aggravent la crise mondiale de la cybersécurité, 21 September 2021
- Trend Micro, CISA Reports Top Vulnerabilities From Remote Work, 21 September 2021
- ZDNet, Siemens Energy launches AI solution to fight industrial cybercrime, 21 September 2021
- APWG – APWG Q2 Cybercrime Report - Phishing Activity Trends, 22 September 2021
- Total Krypto, VEE Finance Under Attack, Lost $35 Million, 22 September 2021
- ICANN, ICANN Launches New IMRS Activity and Incident Report Page, 23 September 2021
- ASPI: ASPI's decades: Cyberattacks, deep fakes and the quantum revolution, 27 September 2021
- Malwarebytes, Demographics of Cybercrime Report, 27 September 2021
- PR Newswire, Global Demographics of Cybercrime Report Reveals Cybercrime Does Not Impact Individuals Equally, 27 September 2021
- Eurojust, Eurojust Written Recommendations on Jurisdiction: Follow-up at the National Level, 29 September 2021
- Eurojust, Eurojust Written Requests on Jurisdiction in a Nutshell, 29 September 2021
- UNODC, UNODC encouraging more women to pursue careers and studies in Cyber, 29 September 2021

Upcoming events

- 4 October-26 November, C-PROC/INTERPOL, (online), E-Evidence Boot Camp (8 weeks E-evidence technical course), including Seminar on the Budapest Convention, GLACY+
- 4-5 October, C-PROC, (online), Regional meeting on online crime proceeds EAP, CyberEast
- 4-6 October, C-PROC/TURKEY, (online), Specialised Judicial Training Course on International Co-operation, iPROCEEDS-2
- 5-7 October, C-PROC/ECUADOR, (hybrid), Cybercrime and money laundering workshop, organized by EL PAaCTO, GLACY+

- 5-8 October, C-PROC/NIGERIA, GHANA, MAURITIUS, (online), Integration of ECTEG training materials and Workshop on LEA training strategies, GLACY+
- 6 October, C-PROC/GHANA, (online), 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 October, C-PROC/NIGERIA, (online), 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 October, C-PROC/BOSNIA and HERZEGOVINA, (online), Domestic workshops on cybercrime and cybersecurity trends as well as for criminal justice statistics in each beneficiary, iPROCEEDS-2
- 7 October, C-PROC/BOSNIA and HERZEGOVINA, Desk assessment, Reports on cybercrime and cybersecurity trends as well as for criminal justice statistics in each beneficiary, iPROCEEDS-2
- 7 October, C-PROC, (online), GFCE Africa Regional Dialogue, GLACY+
- 8 October, C-PROC/MAURITIUS, (online), 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+
- 11 October, C-PROC, (online), Series of webinars on the 2nd Additional Protocol (2/5): Criminal justice cooperation on cybercrime in an emergency situation, in cooperation with International Association of Prosecutors, GLACY+, OCTOPUS
- 12 October, C-PROC/TUNISIA, (online), Second national event on how to elaborate a national report on the evaluation of cyberthreats, CyberSouth
- 12-15 October, C-PROC, (online), Series of first virtual needs assessment meetings in pilot countries: the case for an online training platform, OCTOPUS
- 14 October, C-PROC/LEBANON, (online), Second national event on how to elaborate a national report on the evaluation of cyberthreats, CyberSouth
- 14-15 October, C-PROC, (online), First preparatory meeting for the creation of the Simulation exercise on effective sharing of data between cybercrime and cybersecurity communities, iPROCEEDS-2
- 15 October, C-PROC/MONTENEGRO, (on-line), Online workshop on MLA practices on country level, alignment of procedures with the Budapest Convention and its Second Additional Protocol, iPROCEEDS-2
- October, C-PROC, Desk research, Preparation of country profiles on OCSEA for Brunei, Cambodia, Indonesia, Laos, Malaysia, Singapore, Thailand, Vietnam, OCTOPUS

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 October 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