Cybercrime Digest

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

16 – 31 August 2021

Source: INTERPOL

Date: 16 Aug 2021

INTERPOL issues global alert as fraudsters target governments with COVID-19 vaccine scams

"[…] The warning follows some 60 cases in 40 countries around the world where individuals in health ministries and hospitals have received offers for COVID-19 vaccines approved for distribution in their country. Usually claiming to represent a vaccine manufacturer or a government agency facilitating the distribution of vaccines, the scammers are targeting both professional and personal email accounts of potential buyers, as well as making contact via phone.'' READ MORE

Source: The Irish Times

Date: 24 Aug 2021

Large increase in number of child abuse images investigated by organisation online

"Quarter of reports last year by the public to Hotline.ie, the Irish centre for combatting illegal content online, related to cases involving "hundreds and thousands" of child sexual abuse images and videos. […] The report said 42 per cent of child sexual abuse reports related to content that was indicative of being in commercial nature with Hotline.ie believing that it had been produced or was being used for the purpose of financial gain by the distributor. Last year, the organisation traced child sexual abuse material to 31 countries worldwide, with 56 per cent of the content hosted in Europe." READ MORE

Source: US Department of Justice

Date: 18 Aug 2021

Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million

"[…] the department has disrupted the unlawful money laundering practices of these dangerous criminal enterprises," said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division. "The Justice Department, together with our law enforcement and regulatory partners, will continue to take enforcement actions to identify and impede those who use illicit means for financial gain, as well as those who use the Darknet to facilitate and obscure their criminal conduct. […] The Belize Ministry of the Attorney General and the Belize National Police Department provided essential support for the investigation, coordinated through U.S. Embassy Belmopan. The investigation was coordinated with the Financial Crimes Enforcement Network, which assessed a $60 million civil monetary penalty […].'' READ MORE

Source: Bleeping Computer

Date: 26 Aug 2021

Ragnarok ransomware releases master decryptor after shutdown

"Ragnarok ransomware gang appears to have called it quits and released the master key that can decrypt files locked with their malware. The threat actor did not leave a note explaining the move; all of a sudden, they replaced all the victims on their leak site with a short instruction on how to decrypt files. […] The listed companies are from France, Estonia, Sri Lanka, Turkey, Thailand, U.S., Malaysia, Hong Kong, Spain, and Italy and activate in various sectors ranging from manufacturing to legal services.'' READ MORE

Source: thecrimereport.org

Date: 16 Aug 2021

Feds Offer Dark Web Informants Cryptocurrency for Information on Hackers

"The State Department has launched a new initiative offering up to $10 million to informants with information on state-backed hackers, reports ABC News. For the first time in the Reward for Justice (RFJ) program's almost four decades, informants could elect to receive payments in cryptocurrency and reach out to the US government with sensitive information through a secure portal on the Dark Web. The goal of RFJ's new reward is to solicit helpful information from the type of hackers who might know people involved in state-backed operations." READ MORE

Source: ZDNet

Date: 31 Aug 2021

This phishing attack is using a sneaky trick to steal your passwords, warns Microsoft

"Microsoft has warned Office 365 customers that they're being targeted by a widespread phishing campaign aimed at nabbing usernames and passwords. The ongoing phishing campaign is using multiple links; clicking on them results in a series of redirections that lead victims to a Google reCAPTCHA page that leads to a bogus login page where Office 365 credentials are stolen. […] Microsoft has found over 350 unique phishing domains used in this campaign, including free email domains, compromised domains, and domains automatically created by the attacker's domain generation algorithm." READ MORE

Source: BBC

Date: 20 Aug 2021

Hackers steal nearly $100m in Japan crypto heist

"Leading Japanese cryptocurrency exchange Liquid has been hit by hackers, with almost $100m (£73m) estimated to have been stolen. […] It is the second major theft of cryptocurrencies to take place in recent days. Last week, digital token platform Poly Network was at the centre of a $600m heist. […] Founded in 2014, Liquid operates in over 100 countries and serves millions of customers around the world." READ MORE

RELATED ARTICLE:

Infosecurity Magazine, Poly Network Hacker Returns Remaining Funds, 23 August 2021

Source: Bleeping Computer

Date: 16 Aug 2021

Secret terrorist watchlist with 2 million records exposed online

"A secret terrorist watchlist with 1.9 million records, including classified "no-fly" records was exposed on the internet. The list was left accessible on an Elasticsearch cluster that had no password on it. […] The 1.9 million-strong recordset contained sensitive information on people, including their names, country citizenship, gender, date of birth, passport details, and no-fly status. […]Such databases are regarded as highly sensitive in nature, considering the vital role they play in aiding national security and law enforcement tasks." READ MORE

RELATED ARTICLE:

Welivesecurity, Nearly 2 million records from terrorist watchlist exposed online, 17 August 2021

Source: HackRead

Date: 16 Aug 2021

Hacker selling alleged stolen 100 million T-Mobile customer data for $200

"The hacker claims to have hacked T-Mobile's production, development, and staging servers around two weeks back, including its Oracle database server. […] Over the weekend, the hacking forum's post became the talk of the town after a threat actor claimed to sell databases containing full customer info such as: full names, birth dates, phone numbers, physical addresses, social security numbers, driver's license numbers, security PINs, unique IMSI, IMEI numbers of 30 million customers." READ MORE

RELATED ARTICLE:

Bleeping Computer, T-Mobile says hackers stole records belonging to 48.6 million individuals, 18 August 2021

Source: theprogress newspaper.com

Date: 22 Aug 2021

Gambia, other ECOWAS English speaking countries benefit from GLACY+ Introductory Training Course on Cybercrime for Judges and Prosecutors

"Judges and prosecutors from the ECOWAS English speaking countries – The Gambia, Ghana, Liberia, Nigeria and Sierra Leone recently participated in the Introductory training course on Cybercrime for Criminal Justice Authorities delivered in online format, in an effort to strengthen the judicial capacity of the ECOWAS region and also to ensure sustainability by creating a national pool of experts to train in-country prosecutors and judges on this subject. The training was a collaborative effort between the ECOWAS Commission and the Council of Europe. Both are partnering, through the OCWAR-C and respective GLACY+ projects to support strengthening national and regional judicial capacity in the ECOWAS region through a training programme on cybercrime and electronic evidence." READ MORE

Source: lomebouge.info

Date: 17 Aug 2021

L'ARNAQUE A LA ROMANCE: LE VISAGE DE LA CYBERCRIMINALITE EN AFRIQUE

"Basés plus précisément au Nigéria, au Bénin, au Cameroun, en Côte-d'Ivoire et au Bénin, ces malfaiteurs du net ouvrent des comptes fictifs sur des sites de rencontre, se faisant passer pour des personnes en quête d'amour, certains vont jusqu'à cibler leurs victimes et une fois le contact établi, ils s'échangent des photos et vidéos intimes, objet de chantage pour certains envers leurs victimes si celles-ci ne s'exécutent pas une fois les menaces de publications desdites photos et vidéos émises." READ MORE

Source: aujourdhui.ma

Date: 20 Aug 2021

Cybersécurité: Le Maroc renforce son arsenal juridique

"L'écosystème national de la cybersécurité se consolide. De nouvelles dispositions prennent forme, notamment après l'entrée en vigueur du décret n° 2-21-406 relatif à l'application de la loi n°05-20 relative à la cybersécurité. Ce texte approuvé lors du Conseil des ministres du 28 juin 2021 vise à définir les mesures de protection des systèmes d'information des administrations de l'Etat, des établissements et entreprises publics et toute autre personne morale de droit public, ainsi que ceux des infrastructures d'importance vitale et des opérateurs privés." READ MORE

Source: Daily Maverick

Date: 22 Aug 2021

Russia's efforts to promote cyber norms that serve its interests gain traction in Africa

"Early in July 2021, cyber-attacks originating from Russia prompted US President Joe Biden to call for action from Moscow. This, Biden said, was conveyed to Russian President Vladimir Putin during an hour-long phone call. While the Kremlin denies the US even contacted Moscow about the attacks, recent events have promoted debate around the responsibility of state actors, including Russia, in cyberspace. That country's attempts to promote or resist norms around traditional global governance areas are well documented. It is known to offer a more conservative approach towards issues of human rights and military intervention, for example. And now it is under scrutiny in newer areas of contestation, including cyber governance and cyber security." READ MORE

Source: numerique.gouv.bj

Date: 25 Aug 2021

Sécurité numérique: le Bénin et la Chine signent un mémorandum d'entente

"En marge du Forum de Développement et de coopération Chine-Afrique sur l'Internet (China-Africa Internet and Developement Forum), l'équipe gouvernementale de réponse aux incidents de sécurité informatique au Bénin, le bjCSIRT et son homologue de la Chine, le CNCERT/CC, ont signé le mardi 24 août 2021, un mémorandum d'entente. Pour M. Ouanilo MEDEGAN FAGLA, Directeur Général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI Bénin), la signature de ce mémorandum d'entente s'inscrit dans le cadre de l'objectif spécifique n°5 de la Stratégie Nationale de Sécurité Numérique, intitulé « la coordination nationale et la coopération internationale »" READ MORE

Source: tribuneonlineng.com

Date: 26 Aug 2021

Cybercrimes: 70 per cent of Nigerian youths may soon become ex-convicts

"Economic and Financial Crimes Commission (EFCC) has raised the alarm that more than 70 per cent of Nigerian youths may soon become ex-convicts if the present high rate of their involvement in cybercrime is not stopped. Speaking with journalists in Ilorin, on Thursday, the Ilorin zonal commander of the antigraft agency, Usman Muktar, decried the high rate of cybercrime among youth and enjoined every stakeholder in the country to discourage the youth from internet fraud. Muktar, who said that the EFCC had witnessed an increasing number of arrests of Nigerian youth in cybercrime in recent time, charged parents to ask their children questions about sources of their wealth." READ MORE

Source: Council of Europe

Date: 16-19 Aug 2021

iPROCEEDS-2: Regional meeting on seizing virtual currency

"The iPROCEEDS-2 Joint Project of the European Union and the Council of Europe organized a 4-day training on seizing virtual currency, on 16-19 August 2021, in Bucharest, Romania. The event was physically attended by more than 30 cybercrime and financial investigators, representatives of Financial Intelligence Units and cybercrime prosecutors from the iPROCEEDS-2 project countries/area and Romania and focused on the newly developed Guide on seizing cryptocurrencies." READ MORE

Source: dw.com

Date: 18 Aug 2021

Cuba introduces new cybersecurity law following historic protests

"The Cuban government on Tuesday published decrees spelling out its first cybersecurity law, which has been criticized as an attempt to limit political and civic freedoms on the island. The decrees, which lay out the Caribbean nation's laws against the use of social media or the internet to insult the state or stir up protests, were published in the Official Gazette weeks after Cuba saw the largest protests it has seen in recent years. The protests were fed, in part, by messages on social media." READ MORE

RELATED ARTICLE:

France24, Critics say new Cuba cybersecurity law limits freedom, 18 August 2021

Source: asamblea.gob.sv

Date: 18 Aug 2021

El Salvador: Comisión de Seguridad recoge insumos, entre fiscales y policías, para robustecer ley contra delitos informáticos

"Los diputados de la Comisión de Seguridad y combate a la narcoactividad de la Asamblea Legislativa buscan actualizar la Ley Especial contra los delitos informáticos y conexos, vigente desde 2016, debido a que ha quedado desfasada. También porque los delincuentes están cambiando constantemente su modo de operar y por la necesidad de armonizar y coordinar el trabajo que realizan las diferentes instituciones encargadas de combatir el crimen.'' READ MORE

Source: gadgets360

Date: 31 Aug 2021

VPNs in India Should Be Blocked Permanently Due to Increase in Cybercrimes, Parliamentary Panel Again Urges Government

"The Parliamentary Standing Committee on Home Affairs has once again urged the government to block virtual private networks (VPNs) in India. The committee cited VPN services as a technological challenge that lead to "bypass cybersecurity walls and allow criminals to remain anonymous online". In its report presented to Rajya Sabha regarding the government action on previous concerns, the committee again recommended developing a "coordination mechanism" in collaboration with international agencies to block VPNs permanently. It also asked the Ministry of Home Affairs to strengthen the tracking and surveillance mechanisms to put a check on the use of VPN and the dark Web." READ MORE

Source: The Register

Date: 31 Aug 2021

Bangkok Airways hit by LockBit ransomware attack, loses lotsa data after refusing to pay

"Bangkok Airways has revealed it was the victim of a cyberattack from ransomware group LockBit on August 23rd, resulting in the publishing of stolen data. Bangkok Airways' announcement about the matter came last Thursday, a day after LockBit posted a message on its dark web portal threatening the airline to pay a ransom or suffer a data leak. […] The personal data may have included names, nationalities, gender, phone number, email, address, passport information, travel history, partial credit card numbers and even meal preferences. The Thai regional carrier said no operational or aeronautical security systems were impacted." READ MORE

Source: infosecuritymagazine.com

Date: 16 Aug 2021

Half of US Hospitals Shut Down Networks Due to Ransomware

"Nearly half (48%) of US hospitals have disconnected their networks in the past six months due to ransomware, according to a new study from Philips and CyberMDX. The Perspectives in Healthcare Security Report is based on interviews with 130 IT and cybersecurity hospital executives and biomedical engineers and technicians. The findings revealed the outsized impact ransomware continues to have on healthcare organizations (HCOs) after they battled a surge in attacks during the early months of the pandemic. Respondents who admitted to shutting down networks due to ransomware were a mix of those who did so proactively to avoid a damaging breach and those forced to do so because of severe malware infection." READ MORE

Source: The Register

Date: 31 Aug 2021

Australian powers to spy on cybercrime suspects given green light

"A government bill to create new police powers to spy on criminal suspects online, disrupt their data and take over their accounts has been passed with the support of Labor. The identify and disrupt bill passed the Senate on Wednesday, despite concerns about the low bar of who can authorise a warrant, and that the government failed to implement all the safeguards recommended by the bipartisan joint committee on intelligence and security. The bill creates three new types of warrants to enable the AFP and Australian Criminal Intelligence Commission to modify and delete data, take over accounts and spy on Australians in networks suspected of committing crimes." READ MORE

Source: miragenews.com

Date: 20 Aug 2021

Australian police seize record cryptocurrency amount

"Victoria Police has seized almost $8.5M in cryptocurrency as part of an ongoing investigation into online drug trafficking. Yesterday detectives from the Criminal Proceeds Squad seized cryptocurrency valued at $8.498M at the current exchange rate, which is an Australian law enforcement record. A 31-year-old Kinglake woman and a 30-year-old Preston man were arrested and interviewed by police. Both have been released pending further enquiries in relation to this investigation, with the woman charged with possess cannabis." READ MORE

Source: observador.pt

Date: 30 Aug 2021

Portugal: Tribunal Constitucional chumba lei do cibercrime

"O Tribunal Constitucional chumbou a lei do cibercrime, avançou o semanário Expresso. A lei, que tinha sido proposta pelo Governo e aprovada no parlamento pelo PS, PSD, BE e PAN, dava ao Ministério Público o poder de aceder a comunicações eletrónicas privadas em investigações de cibercrime, sem autorização prévia de juízes. A informação foi posteriormente corroborada pela agência Lusa, que indicou que o Tribunal Constitucional declarou por unanimidade a inconstitucionalidade da lei. Os dois órgãos citam o acórdão da conselheira Mariana Canotilho, em que se considerou que estava em causa uma "restrição dos direitos fundamentais à inviolabilidade da correspondência" e uma "violação das garantias constitucionais de defesa em processo penal." READ MORE

Source: zdnet.com

Date: 26 Aug 2021

Data protection: UK to diverge from GDPR in post-Brexit overhaul of privacy rules

"The UK has announced plans to change data protection and privacy laws in what the government describes as a new mandate that promotes innovation and economic growth. A new series of 'data adequacy partnerships' will allow Britain to drive international trade with countries and bodies including the United States, Australia, the Republic of Korea, Singapore, the Dubai International Finance Centre and Colombia, the Department for Digital, Culture, Media & Sport (DCMS) has said. According to the government, the data adequacy partnerships will remove the need for costly measures around data compliance when transferring personal data to other countries." READ MORE

Latest reports

- EUROPOL, Online Jihadist Propaganda - 2020 in review, 13 August 2021
- Konrad Adenauer Stiftung, La ciberseguridad en México, ¿una necesidad?, 16 August 2021
- Aic.gov, Responding to cybercrime: Results of a comparison between community members and police personnel, 19 August 2021
- Web Hosting Rating, 40+ Cybersecurity Statistics & Facts For 2021, 18 August 2021
- Talos, Malicious Campaign Targets Latin America: The seller, The operator and a curious link, 19 August 2021
- Circle ID, The Bright Side of Decentralized Domain Names, 20 August 2021
- Undernews.fr, Aperçu des cybermenaces mondiales au T2 2021, 20 August 2021
- Zix, 2021 Mid-Year Global Threat Report, 22 August 2021
- Just Security, International Law's Role in Combating Ransomware?, 23 August 2021
- BuyShares, 40% of Businesses Feel Threatened by Cyber Incidents in 2021, 23 August 2021
- Just Security, International Law's Role in Combating Ransomware?, 23 August 2021
- Circle ID, DNS Abuse Definition: Attributes of Mitigation, 24 August 2021
- Harvard Kennedy School, Cybercrime Hotspots, Identifying the Conditions that Influence the Emergence of Financially-Motivated Cybercriminal Networks, 24 August 2021
- PYMNTS, Cybersecurity Czar Richard Clarke Tells PYMNTS 'New Mindset' Needed To Win Cyberwar, 24 August 2021
- Belfer Center, Cybercrime Hotspots - Identifying the Conditions that Influence the Emergence of Financially-Motivated Cybercriminal Networks, 24 August 2021
- IPleaders, Six most common types of phishing attacks and how to prevent them, 24 August 2021
- Digital Information World, Over 304 million ransomware threats surfaced in the first half of 2021, 25 August 2021
- Honeywell Survey: 71% Of Surveyed Facility Managers State Concerns About Operational Cybersecurity, 25 August 2021
- Circle ID, To Block or Not to Block?, 29 August 2021
- Cybersecurity and Infrastructure Security Agency (CISA)- Ransomware Awareness for Holidays and Weekends, 31 August 2021
- Forbes, Ransomware: What's Next In 2021? 31 August 2021
- Asian Development Bank, E-Commerce in CAREC Countries: Laws and Policies, August 2021
- Canadian Global Affairs Institute, Debt, Tech and Tension: Addressing COVID-19's Global Fault Lines, August 2021

Upcoming events

- September – December 2021, Desk review, Update of the Electronic Evidence Guide of the Council of Europe, iPROCEEDS-2
- 6 – 9 September, C-PROC/Armenia (online), Pilot session of online judicial training, CyberEast
- 7-8 September, Paraguay (online), Advisory workshop on integration/ mainstreaming of training modules in curricula of judicial training institutions and prosecutors' training institution, GLACY+
- 7 – 9 Sepetmber, Kosovo*[1] (online), Simulation exercise for developing skills on cooperation on cybercrime and electronic evidence for judicial, police and cybersecurity authorities with service providers, iPROCEEDS-2
- 10 September, C-PROC/Azerbaijan (online), Workshop with Azerbaijani authorities on cybercrime/cybersecurity strategy and action plan (with CyberSecurity EAST project), CyberEast
- 13 – 17 September, online, SCENARI training provided by ECTEG under the Translation of the first responder training course, E-FIRST, iPROCEEDS-2
- 14 – 16 September, Bosnia and Herzegovina (online), Simulation exercise for developing skills on cooperation on cybercrime and electronic evidence for judicial, police and cybersecurity authorities with service providers, iPROCEEDS-2
- 14-16 September, C-PROC/Armenia (online), Effective access to data exercise on cooperation between LEA/ISPs, CyberEast
- 14-17 September, Mauritius (online), Cryptocurrency basics, implemented with the assistance of GLACY+ partner – INTERPOL.

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, some in-country activities of the C-PROC capacity building initiatives foreseen in the month of August 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

[1] *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.