Cybercrime Digest

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

16 – 31 July 2021

Source: European Commission

Date: 20 Jul 2021

Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules

"The European Commission has today presented an ambitious package of legislative proposals to strengthen the EU's anti-money laundering and countering terrorism financing (AML/CTF) rules. […] Today's measures greatly enhance the existing EU framework by taking into account new and emerging challenges linked to technological innovation. […] At present, only certain categories of crypto-asset service providers are included in the scope of EU AML/CFT rules. The proposed reform will extend these rules to the entire crypto sector, obliging all service providers to conduct due diligence on their customers. Today's amendments will ensure full traceability of crypto-asset transfers, such as Bitcoin, and will allow for prevention and detection of their possible use for money laundering or terrorism financing. In addition, anonymous crypto asset wallets will be prohibited, fully applying EU AML/CFT rules to the crypto sector." READ MORE

RELATED ARTICLE:

CSO, EU takes aim at ransomware with plans to make Bitcoin traceable, prohibit anonymity, 23 July 2021

Source: Council of the European Union

Date: 19 Jul 2021

China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory

"Today, the EU and its member states, together with partners, expose malicious cyber activities that significantly affected our economy, security, democracy and society at large. The EU and its member states assess these malicious cyber activities to have been undertaken from the territory of China. […] The EU and its member states strongly denounce these malicious cyber activities, which are undertaken in contradiction with the norms of responsible state behaviour as endorsed by all UN member states. We continue to urge the Chinese authorities to adhere to these norms and not allow its territory to be used for malicious cyber activities […]." READ MORE

Source: Radio New Zealand

Date: 20 Jul 2021

Government points finger at China over cyber attacks

"The government says it has uncovered evidence of Chinese state-sponsored cyber attacks in New Zealand. GCSB Minister Andrew Little said that the foreign intelligence agency has established links between Chinese state-sponsored actors known as Advanced Persistent Threat 40 (APT40) and malicious cyber activity in New Zealand.[…] He said the government is joining other countries in strongly condemning what the Chinese Ministry of State Security has been doing both in New Zealand and globally." READ MORE

Source: ZD Net

Date: 30 Jul 2021

Ransomware attempt volume sets record, reaches more than 300 million for first half of 2021

"The US, UK, Germany, South Africa and Brazil topped the list of countries most impacted by ransomware attempts while states like Florida and New York struggled as well. […] The report notes that the ransomware problem continues to worsen, and the data proved that Q2 was far worse than Q1 for 2021. Q2 was the worst quarter ever recorded by the company, with a ransomware volume of 188.9 million, far surpassing the Q1 figure of 115.8 million. […] The report did include some good news. The volume of malicious PDF files and Office files dropped for the first time since 2018. Malware targeting IoT skyrocketed in 2021 with more than 32 million attacks, and in the US attempts on IoT increased by 15%." READ MORE

Source: Europol

Date: 26 Jul 2021

UNHACKED: 121 tools against ransomware on a single website, 26 July 2021

"The decryptors available in the No More Ransom repository have helped more than six million people to recover their files for free. This prevented criminals from earning almost a billion euros through ransomware attacks. Currently offering 121 free tools able to decrypt 151 ransomware families, it unites 170 partners from the public and private sector. The portal is available in 37 languages." READ MORE

Source: Interpol

Date: 21 Jul 2021

INTERPOL Victim Identification task force focuses on Asian victims

"A number of investigations have been generated following an INTERPOL Victim Identification Task Force gathering specialized officers from 11 Asia Pacific countries, in a targeted effort to identify victims and offenders depicted in child sexual exploitation material. Officers from Australia, Bangladesh, Cambodia, India, Indonesia, Malaysia, Maldives, Philippine Singapore, Sri Lanka and Vietnam spent two intensive weeks in early July analysing material selected by INTERPOL's Crimes against Children (CAC) unit depicting yet unknown victims." READ MORE

Source: Europol

Date: 29 Jul 2021

Russian-speaking hackers arrested in Poland over ATM jackpotting attacks

"With the support of Europol, the Polish authorities have arrested two individuals committing so-called 'Black Box' attacks against ATMs, in which criminals connect electronic devices to a cash machine and remotely force it to spew out all its cash. […] The investigation uncovered that these criminals committed dozens of ATM attacks in at least seven European countries, stealing an estimated €230 000 in cash. The criminals were always targeting the same brand and model of ATM." READ MORE

Source: FE News

Date: 29 Jul 2021

Fresh data shows a 600% rise in education-related cybercrime

"With high-profile attacks against established technology and infrastructure, ransomware is now more prevalent than ever. […] In line with spikes in global data, SonicWall Capture Labs threat researchers also recorded alarming ransomware spikes across key verticals, including government (917%), education (615%), healthcare (594%) and retail (264%) organizations." READ MORE

Source: US Department of Justice

Date: 21 Jul 2021

Man Arrested in Connection with Alleged Role in Twitter Hack

"A citizen of the United Kingdom was arrested today in Estepona, Spain, by Spanish National Police pursuant to a U.S. request for his arrest on multiple charges in connection with the July 2020 hack of Twitter that resulted in the compromise of over 130 Twitter accounts, including those belonging to politicians, celebrities and companies. [...] The Justice Department's Office of International Affairs is providing significant assistance. The U.K.'s National Crime Agency and the Spanish National Police provided assistance in the investigation and arrest." READ MORE

RELATED ARTICLE:

The Verge, PlugWalkJoe' arrested in connection with 2020 hack of famous Twitter accounts, 21 July 2021

Source: Trilateral Research

Date: 22 Jul 2021

Child sexual exploitation online: how can we better protect children in the wake of COVID-19 lockdowns?

"While some parents have converted to working from home, children are experiencing more unsupervised access to the internet which potentially results in – as argued by EUROPOL – more exposure to offenders and also potentially higher risk of becoming lonely and isolated. This sentiment is also echoed by the Internet Watch Foundation (IWF), who contend that there has been a considerable increase in child sexual imagery since the beginning of the pandemic lockdown." READ MORE

Source: Mundo en linea

Date: 20 Jul 2021

¿Cuáles son las modalidades de ciberataque más frecuentes en América Latina?

"Un informe de la plataforma Threat Intelligence Insider Latin America, de Fortinet, señala que durante el primer semestre de 2020 Latinoamérica y el Caribe fueron víctimas de 15.000 millones de intentos de ciberataques, de los cuales 525 millones acontecieron en Chile. Las empresas, de acuerdo con la publicación, figuran como el principal blanco de ataque. […] A partir de la experiencia de TIVIT, los principales objetivos de los ciberataques en la región son la ganancia financiera (33%), la interrupción del servicio (31%) y el robo de datos (22%)." READ MORE

Source: Council of Europe

Date: 22-23 Jul 2021

Octopus Project: Authorities in Barbados are pursuing updates of their domestic cybercrime legislation in line with the Budapest Convention

"National authorities of Barbados are invested in updating their domestic legislation on cybercrime and electronic evidence in line with the provisions of the Budapest Convention as the international legislative standard in the field. […] a preparatory meeting took place online on 22-23 July with the participation of representatives from the Law Reform Commission and the Chief Parliamentary Counsel's Office. The purpose of the meeting was to have a more detailed discussion on amendments recommended to be made in line with international standards." READ MORE

Source: El País Uruguay

Date: 31 Jul 2021

Uruguay: Boom de extorsiones sexuales y estafas online: ¿cómo frenar los ciberdelitos?

"Las extorsiones por contenidos sexuales, las estafas y la pornografía infantil están detrás de la mayoría de las investigaciones que realiza el Departamento de Delitos Informáticos del Ministerio del Interior. En 2020 recepcionó 1.700 denuncias y en 2021 ya superan las 800. […] Sumarse al Convenio de Budapest permitiría "agilizar" las investigaciones, ya que habría un mejor intercambio de información entre los países miembros (en vez de recurrir a los exhortos, que son más lentos) y "aumentaría el margen" para que las empresas de redes sociales respondan las solicitudes de información más seguido y a más delitos de los que suelen responder, que son el terrorismo, la pornografía infantil y las amenazas de muerte." READ MORE

RELATED ARTICLE:

Crónicas, Cuando la tecnología desafía los límites: proyecto de ley sobre ciberdelitos, 23 July 2021

Source: CoinDesk

Date: 24 Jul 2021

Brazilian Police Seize $33M in Crypto Money Laundering Probe

"Brazil's civil police seized R$172 million (US$33 million) amid an investigation into money laundering carried out through crypto exchanges. During an operation known as "Exchange" that took place in Sao Paulo and Diadema, Brazilian police carried out six search warrants, after which the Brazilian judiciary authorized freezing accounts and seizing assets from two individuals and 17 companies, according to an official statement that did not name them. The investigation found that crypto exchanges acquired and sold bitcoin to fictitious companies fabricated to facilitate their creators' access to the banking system." READ MORE

Source: El Popular

Date: 25 Jul 2021

México, de los países más vulnerables a la ciberdelincuencia

"México debe mejorar sus estándares de seguridad cibernética y controles técnicos, además del desarrollo de un mercado de ciberseguridad para reducir los estragos de los ciberataques, consideró la Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Josefina Román Vergara." READ MORE

Source: The Zimbabwe Independent

Date: 30 Jul 2021

Zimbabwe: Cyber Security Bill sails through

"The Cyber Security and Data Protection Bill on Wednesday sailed through the Senate without debate, but media lobby groups have immediately expressed wary over the potential abuse of the law by the government to trample on people's rights to information. Its provisions have been subjected to widespread criticism on the grounds that it violates fundamental rights such as the right to privacy, the right to freedom of speech and the right to access to information. The Bill, which now awaits Presidential assent to make it law, will regulate the use of the internet and social media activities to curb computer crimes such as spreading of pornographic content, and other internet related financial fraudulent activities, including criminalizing child-pornography." READ MORE

Source: Council of Europe

Date: 20-22 Jul 2021

Angola virtually hosts the annual forum of the FIU of the Portuguese Speaking African Countries (PALOP) and East Timor

"The Financial Intelligence Unit (FIU) of Angola, celebrating 10 years of activity in 2021, in collaboration with the European Union project to support the consolidation of the rule of law in PALOP and Timor-Leste (PACED) and the GLACY+ project hosted, between 20 and 22 July, the annual forum of the FIUs of the Portuguese Speaking African Countries (PALOP) and East Timor. The forum focused on "Streamlining parallel financial investigation in cybercrime cases: trends and challenges" READ MORE

Source: News 24

Date: 28 Jul 2021

South Africa: Cybercrime is a life-threatening emergency – it must be stopped

"The signing of the Cybercrimes Act into law by President Cyril Ramaphosa in June was a good start that will require intensified and coordinated action to materialise. […] South Africa must work with fellow African states to marshal all resources to deal with this form of crime. In doing so, we fortunately might be able to count on international agencies to support our initiatives. The African Continental Free Trade Area (AfCFTA) agreement provides a further incentive to really step on the gas." READ MORE

Source: Evening Standard

Date: 22 Jul 2021

'Substantial' rise in fraud and hacking during coronavirus pandemic

"Fraud and hacking soared during the pandemic as criminals "took advantage of behavioural changes" while reports of domestic abuse-related offences also rose, official figures show. Lockdowns and restrictions in movement in England and Wales saw a surge in online shopping which led to "substantial increases" in computer crimes, according to the Office for National Statistics (ONS).[…] Action Fraud, the national fraud and cybercrime reporting centre, reported a 28% rise in fraud offences, from 312,035 in 2019/20 to 398,022 in 2020/21." READ MORE

RELATED ARTICLE:

UK Office for National Statistics, Crime in England and Wales: year ending March 2021, 29 July 2021

Latest reports

- EUROJUST, The impact of COVID-19 on judicial cooperation in criminal matters - Executive summary of information compiled by Eurojust and EJN, 16 July 2021
- CISA, Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department, 19 July 2021
- ECHR, Judgment Akgun v. Turkey - pre-trial detention of an applicant suspected of FETÖ/PDY membership: violation of the Convention, 20 July 2021
- EUROJUST, European Judicial Cybercrime Network 10th Plenary Meeting - Outcome summary, 21 July 2021
- HP Wolf Security, HP Wolf Security Threat Insights Report 1H 2021, 21 July 2021
- Crowdfun Insider, Kaspersky Report Parses African Cybercrime Trends, 21 July 2021
- ENISA, Telecom & Trust Services Incidents in 2020: System Failures on the Rise, 26 July 2021
- Fugue, The State of Cloud Security 2021 Report, 27 July 2021
- Save the Children, Little invisible slaves, 28 July 2021
- Kaspersky, DDoS attacks in Q2 2021, 28 July 2021
- ENISA, Threat Landscape for Supply Chain Attacks, 29 July 2021
- Check Point Research, Cyber Attack Trends: 2021 Mid-Year Report, 29 July 2021
- Sonic Wall, Mid-year update Sonicwall cyber threat Report, 29 July 2021
- Kaspersky, APT trends report Q2 2021, 29 July 2021

Upcoming events

- 3 August, C-PROC/BOSNIA&HERZEGOVINA, (online), Workshop on MLA practices at country level, alignment of procedures with the Budapest Convention and its Second Additional Protocol, iPROCEEDS-2
- 3 August, C-PROC / SOUTH AFRICA, (online), Workshop on benchmarking of the implementation of the South African Cybercrimes Act, SA-EU Dialogue Facility in cooperation with Octopus
- 3 - 6 August, C-PROC/COSTA RICA, (online), Specialized Course on International Cooperation for prosecutors and judges, GLACY+
- 10 August, C-PROC/NIGERIA, GHANA, MAURITIUS, (online), Integration of ECTEG training materials and Workshop on LEA training strategies, GLACY+
- 11 August, 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+
- 12 August, 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+
- August-September, C-PROC (online), Development of training on interagency cooperation and financial investigations/intelligence, CyberEast and GLACY+

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 August 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