Cybercrime Digest

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

01 – 15 July 2021

Source: Euractiv

Date: 06 July 2021

New EU law allows screening of online messages to detect child abuse

"The European Parliament adopted on Tuesday (6 July) the final version of the ePrivacy derogation, a temporary measure enabling providers of electronic communication services to scan and report private online messages containing material depicting child sex abuse. […] The new regulation provides a legal framework for tech companies to monitor interpersonal communications on a voluntary basis with the purpose of detecting and reporting material depicting sexual abuse of minors or attempts to groom children." READ MORE

RELATED ARTICLE:

Draft European Parliament legislative resolution on the temporary derogation from certain provisions of Directive 2002/58/EC

Source: Council of Europe

Date: 08 July 2021

The International Network of National Judicial Trainers: second series of Practitioners-to-Practitioners workshops starting September

"On 08 July, the International Network of National Judicial Trainers concluded the first series of six practitioners-to-practitioners workshops, as part of the current efforts to enable judges and prosecutors to enhance their knowledge on cybercrime and electronic evidence through training, networking and specialization. […] For the upcoming series, we welcome any further expression of interest for presentations from members of the Network. Hence, those interested in presenting, are invited to fill in our International Network of Judicial Trainers form, available in English, French, Spanish and Portuguese." READ MORE

Source: EUROJUST

Date: 08 July 2021

New action against online criminal network defrauding users of popular consumer sites

"Eurojust has coordinated a follow-up action against a Romanian criminal network involved in extensive online fraud against users of popular consumer sites such as Amazon and eBay. During an action day, the Romanian and Greek authorities arrested eight members of an organised crime group (OCG). The criminal network used phishing scams to defraud online customers of at least EUR 2 million as they tried to buy prestigious cars and a range of other products, or to book accommodations. In total 30 places were searched and EUR 220 000 in cash, mobile phones and travel documents were seized." READ MORE

Source: INTERPOL

Date: 12 July 2021

Immediate action required to avoid Ransomware pandemic

"INTERPOL Secretary General Jürgen Stock has called for police agencies worldwide to form a global coalition with industry partners to prevent a potential ransomware pandemic. Speaking at the INTERPOL High-Level Forum on Ransomware (12 July), Secretary General Stock said that while some solutions existed nationally or bi-laterally, effectively preventing and disrupting ransomware meant adopting the same international collaboration used to fight terrorism, human trafficking or mafia groups such as the 'Ndrangheta. READ MORE

Source: Eucrim

Date: 09 July 2021

Commission Recommends Joint Cyber Unit

"Despite major progress in achieving cybersecurity – i.e., through cooperation between Member States and relevant EU institutions, bodies, and agencies (EUIs) and by means of the existing legislative framework – there is still no common EU platform where information gathered in different cybersecurity communities can be exchanged. […] In order to fill this gap and coordinate the EU effort against cyber-threats, incidents, and crises, the Commission has developed a concept for a Joint Cyber Unit that will offer coordinated assistance to Member States and EUIs in times of crisis." READ MORE

RELATED ARTICLE:

European Commission, Recommendation on building a Joint Cyber Unit, 23 June 2021

Source: Reuters

Date: 06 July 2021

Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says

"Between 800 and 1,500 businesses around the world have been affected by a ransomware attack centered on U.S. information technology firm Kaseya, its chief executive said on Monday. […] One of those tools was subverted on Friday, allowing the hackers to paralyze hundreds of businesses on all five continents." READ MORE

RELATED ARTICLE:

ZD Net, Kaseya ransomware attack: 1,500 companies affected, company confirms, 06 July 2021

Source: World Economic Forum

Date: 07 July 2021

Only cross-border, cross-sector collaboration will be enough to beat cybercrime

"[…] Ransomware has become a top threat to international security and a global challenge requiring a coordinated response. As institutions across sectors increasingly become targets, a single attack can rapidly spread across borders, much like the 2017 WannaCry ransomware attack that affected 150 countries. It is expected that the impact of such an attack in 2021 could be even more severe leading to vast losses, devastating blows to critical infrastructure, and the generation of further funding for illegal activities. […] In order to tackle the vulnerability of the ecosystem, a fundamental shift towards a collective response is needed from society, government and organizations. Only through such a coordinated approach can we hope to turn the tide of these attacks." READ MORE

Source: ZD Net

Date: 01 July 2021

Facebook, Google, TikTok, Twitter promise a safer space for women online

"Facebook, Google, TikTok, and Twitter have vowed to improve women's safety on their respective platforms, agreeing to a set of commitments during the United Nations Generation Equality Forum. The commitments focus on improving systems for reporting abuse and offering features that give women more control over their online experience. They were developed as part of a year-long initiative led by the World Wide Web Foundation. The foundation worked with 120 people comprised of experts from various tech companies, governments, and civil society as well as women who have been affected by online abuse. In total, 35 countries were represented." READ MORE

Source: ITahora

Date: 06 July 2021

La AECI impulsa la participación de Ecuador en el Convenio de Budapest

"La Asociación Ecuatoriana de Ciberseguridad, AECI está impulsando que Ecuador sea parte del convenio de Budapest. Este convenio que entró en vigor en 2004 establece una política penal común y de cooperación internacional para hacer frente a los delitos informáticos. […] Para la AECI, es importante que Ecuador se suscriba y adhiera al convenio de manera que se cuente con una herramienta común para procesar las manifestaciones delictivas y permita el mejoramiento de la cooperación internacional de los países suscriptores del convenio. […] En este pedido, la AECI insta a que la Asamblea Nacional o el Poder Ejecutivo del país inicie de forma inmediata la adopción del Convenio." READ MORE

Source: Agencia Brasil

Date: 08 July 2021

Brazil: Polícias de nove estados fazem operação de combate a crimes digitais

"Sob a coordenação da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública (MJSP), foi deflagrada, nesta quinta-feira (8), a terceira fase da Operação 404, com o objetivo de combater crimes de pirataria digital. As ações estão executadas pelas Polícias Civis de nove estados: Espírito Santo, Maranhão, Mato Grosso, Mato Grosso do Sul, Pará, Pernambuco, Rondônia, Rio Grande do Sul e São Paulo. " READ MORE

Source: WeLiveSecurity

Date: 07 July 2021

Bandidos at large: A spying campaign in Latin America

"In 2021 we detected an ongoing campaign targeting corporate networks in Spanish-speaking countries, with 90% of the detections in Venezuela. When comparing the malware used in this campaign with what was previously documented, we found new functionality and changes to this malware, known as Bandook. We also found that this campaign targeting Venezuela, despite being active since at least 2015, has somehow remained undocumented. […] Previous reports have mentioned that the developers of Bandook might be developers for hire (also known as "malware as a service"), which makes sense given the various campaigns with different targets seen through the years." READ MORE

Source: ECOWAS

Date: 13 July 2021

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

"The ECOWAS Commission and the Council of Europe 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. Judges and prosecutors from the ECOWAS English speaking countries […] have 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." READ MORE

RELATED ARTICLE:

Council of Europe, GLACY+: Introductory Training Course on Cybercrime for Judges and Prosecutors from ECOWAS English speaking countries, 05-08 July 2021

Source: INTERPOL

Date: 06 July 2021

Moroccan police arrest suspected cybercriminal after INTERPOL probe

"[…] Under Operation Lyrebird, INTERPOL's Cybercrime Directorate worked closely with Group-IB and with Moroccan Police via the INTERPOL National Central Bureau in Rabat to eventually locate and apprehend the individual who remains under investigation. INTERPOL Executive Director of Police Services Stephen Kavanagh said: "This is a significant success against a suspect who is accused of targeting unsuspecting individuals and companies across multiple regions for years, and the case highlights the threat posed by cybercrime worldwide." […] In May INTERPOL launched a new cyber operations desk to boost the capacity of 49 African countries to fight cybercrime." READ MORE

Source: Council of Europe

Date: 28 June – 02 July 2021

GLACY+: Cybercrime First Responders Training for the African Gendarmerie Officers

"[…] The online course was delivered to approximately 30 officers coming from 16 member countries of the African Gendarmerie Organisation including Burkina Faso, Cameroon, Chad, Congo, Cote d'Ivoire, Djibouti, Equatorial Guinea, Gabon, Guinea, Madagascar, Mali, Mauritania, Niger and Togo and also 20 officers coming from Senegal. The GLACY+ Project will continue to support the country in its future endeavours to train officers who come into contact with cybercrime or electronic evidence in the course of their duties." READ MORE

Source: Council of Europe

Date: 13 July 2021

CyberSouth: National Workshop for supporting the establishment of the 24/7 Contact Point in Tunisia

"In order to assist the Tunisian authorities to complete the process for accession to the Budapest Convention and following their request, a meeting on the establishment of 24/7 Contact Point (CP) took place, online, on the 13th of July 2021. This workshop follows the previous advisory mission on the role of the 24/7 CP implemented by the CyberSouth project on the 27th of August 2018." READ MORE

Source: Council of Europe

Date: 30 June – 7 July 2021

iPROCEEDS-2: Online workshops on handling electronic evidence during the investigation and prosecution of cybercrimes in Turkey

"Within the framework of Joint European Union and Council of Europe iPROCEEDS-2 and Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of the European Convention on Human Rights Violations in Turkey projects, two one-day online workshops on handling of evidence and electronic evidence during the investigation and prosecution of cybercrimes have been organised on 30 June 2021 and 07 July 2021, for judges and prosecutors in Turkey." READ MORE

Source: Guru3d

Date: 04 July 2021

Ukraine Security Service Shuts Down Illegal Crypto Farm With 3800 PS4 Consoles Sucking 200k electricity monthly

"The security service of the Ukrainian (SBI) shut down a mining farm holding 3800 PS4 Consoles. The crypto miners exploited a deserted warehouse there and used energy to mine bitcoins from the electricity system in the city. The perpetrators illegally used the electricity network. According to the authorities, the monthly costs would amount to a maximum of 7 million Ukrainian hryvnia, converted to about 215,000 euros. […] The Security Service of Ukraine discovered the illegal mining operation and reported that more than 50 processors, 500 graphics cards, and 3,800 PlayStation 4 consoles were seized in a raid." READ MORE

Source: US Department of Justice

Date: 15 July 2021

U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov

"[…] as part of the ongoing response, agencies across the U.S. government announced new resources and initiatives to protect American businesses and communities from ransomware attacks. The U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS), together with federal partners, have launched a new website to combat the threat of ransomware. StopRansomware.gov establishes a one-stop hub for ransomware resources for individuals, businesses and other organizations." READ MORE

Source: EUROPOL

Date: 02 July 2021

Six children victim of sexual abuse removed from harm as a result of Europol's victim identification taskforce

"Six victims of child abuse have been identified and removed from harm as a result of the 9th Victim Identification Taskforce organized by Europol's European Cybercrime Centre (EC3). […] Europol is managing more than 59 million unique images and video files in its dedicated repository. To prepare for the action, Europol specialists selected footage of victims whose location and identity had not yet been established." READ MORE

Source: Vie publique

Date: 04 July 2021

Cybersécurité des entreprises : comment mieux protéger les TPE et les PME ?

"Le développement du e-commerce depuis quelques années et le recours massif au télétravail, du fait de la crise sanitaire ces derniers mois, ont accru les risques de cyberattaques. Un rapport d'information relatif à la cybersécurité des entreprises, remis au Sénat le 10 juin 2021, dresse le bilan de cette menace et de sa prise en compte par les entreprises et les pouvoirs publics. Face à ce constat, le rapport propose également un certain nombre de réponses afin de mieux aider les TPE et les PME à faire face à la cybercriminalité." READ MORE

Source: The Hacker News

Date: 14 July 2021

16 Cybercriminals Behind Mekotio and Grandoreiro Banking Trojan Arrested in Spain

"Spanish law enforcement agencies on Wednesday arrested 16 individuals belonging to a criminal network in connection with operating two banking trojans as part of a social engineering campaign targeting financial institutions in Europe. […] Computer equipment, mobile phones, and documents were confiscated, and more than 1,800 spam emails were analyzed, enabling law enforcement to block transfer attempts totaling €3.5 million successfully. The campaign is said to have netted the actors €276,470, of which €87,000 has been successfully recovered." READ MORE

Source: BBC News

Date: 13 July 2021

Met Police seize record £180m of cryptocurrency in London

"The Met Police has seized a record £180m worth of cryptocurrency linked to international money laundering in London. The seizure is the largest of its kind in the UK - beating the previous record set when the Met confiscated £114m of cryptocurrency on 24 June. The Met's economic crime command made the seizure after following up intelligence received about the transfer of criminal assets. The investigation is continuing." READ MORE

Latest reports

- ITU, Global Cybersecurity Index, June 2021
- NSA, NSA, Partners Release Cyber security Advisory on Brute Force Global Cyber Campaign, 01 July 2021
- Council of Europe, The global state of cybercrime legislation 2013 – 2021: A cursory overview, 02 July 2021
- WeLiveSecurity, Kaseya supply-chain attack: What we know so far, 03 July 2021
- Eurojust, Eurojust Guidelines on How to Prosecute Investment Fraud, 05 July 2021
- Enisa, 5G Supplement - to the Guideline on Security Measures under the EECC, 07 July 2021
- State Watch, EU: Outgoing Portuguese Presidency report on "e-evidence" state of play, 08 July 2021
- Tech Monitor, The evolution of ransomware extortion tactics, 12 July
- Rappler, Holding the world to ransom: the 5 most dangerous criminal organizations online right now, 12 July 2021
- Help Net Security, IT, healthcare and manufacturing top targets for cyberattacks, 12 July 2021
- Cellebrite, 2021 Digital Intelligence Benchmark Report: Despite Lockdown Drop in Crime, Investigations Still Slowed by Digital Evidence, 14 July 2021
- ScienceDirect, Digital evidence in fog computing systems, July 2021

Upcoming events

- 20-22 July, C-PROC/PALOP COUNTRIES & TIMOR LESTE, (on-line), Streamlining parallel financial investigation in cybercrime cases. Trends and challenges, GLACY+
- 22-23 July 2021, C-PROC/BARBADOS (online), advisory mission on legislation on cybercrime and electronic evidence, Octopus project in cooperation with CARICOM IMPACS
- 26-30 July, C-PROC/AFRICA, INTERPOL Malware Analysis Training (Africa, Europe and Middle East), GLACY+
- 27-29 July, C-PROC/ SERBIA (on-line), Domestic/online practical exercise bringing together cybercrime, cybersecurity and the private sector aimed at developing practical skills of public-private cooperation, iPROCEEDS-2
- 28-29 July, C-PROC/COLOMBIA, (on-line), INTERPOL, Development of Cybercrime investigations, digital forensics capabilities combined with in-country workshops and advice on interagency cooperation and private public partnerships to fight cybercrime, GLACY+
- By 31 July (Date TBC), C-PROC, Desk Assessment, Global survey on the state of play of the judicial training (under the framework of the International Network of Judicial Trainers), GLACY+
- By 31 July (Date TBC), C-PROC/BURKINA FASO, (on-line), Advisory mission on legislation, GLACY+
- By 31 July 2021, C-PROC, setting up of the proof of concept version of the online training platform on cybercrime, Octopus
- By 31 July 2021, C-PROC, preparation of the high-level review on legislation on OCSEA in Asia region, 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 July 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