Cybercrime Digest

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

01 – 18 November 2021

Source: Council of Europe

Date: 17 Nov 2021

Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe

"As the Convention on Cybercrime turns 20, the Committee of Ministers of the Council of Europe has adopted a Second Additional Protocol to the Convention on enhanced co-operation and the disclosure of electronic evidence. [...] Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement are limited by territorial boundaries. [...] As a response, the Protocol provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards. The text should be opened for signature in May 2022." READ MORE

Source: Council of Europe

Date: 18 Nov 2021

Octopus Conference 2021: key messages

"About 1200 cybercrime experts from some 120 countries – including from public sector but also international and private sector organisations, civil society organisations and academia – participated in the Octopus Conference on Cybercrime from 16 to 18 November 2021. The conference commenced on 16 November with a special event on the occasion of the 20th anniversary of the Budapest Convention on Cybercrime and on the forthcoming Second Additional Protocol to the Convention on enhanced cooperation and disclosure of electronic evidence. […] Interventions by ministers, prosecutors general and other senior officials from all regions of the world confirmed the global impact and benefits of the Convention and the need for the new Protocol. Octopus 2021 was the 13th edition of this conference. The bottom line of all the previous ones had been a call to "cooperate". The one for Octopus 2021 is the same but includes a supplement: cooperate, the tools are there!" READ MORE

Source: Council of Europe

Date: 9 Nov 2021

Council of Europe marks 20 years of action against cybercrime

"Twenty years after it was adopted, the Budapest Convention remains the most relevant international treaty that protects individuals and their rights against crime online. [...] The Convention has had a global impact. It has helped strengthen and harmonise countries' legislation on cybercrime, enhance the effectiveness of international co-operation in investigating and prosecuting crimes committed via the Internet, and to foster partnerships between the public and private sectors." READ MORE

RELATED ARTICLE:

Direction informatique, La Convention de Budapest sur la cybercriminalité a 20 ans, 11 Nov 2021

Source: Europol

Date: 8 Nov 2021

Five affiliates to Sodinokibi/REvil unplugged

"On 4 November, Romanian authorities arrested two individuals suspected of cyber-attacks deploying the Sodinokibi/REvil ransomware. They are allegedly responsible for 5 000 infections, which in total pocketed half a million euros in ransom payments. Since February 2021, law enforcement authorities have arrested three other affiliates of Sodinokibi/REvil and two suspects connected to GandCrab. These are some of the results of operation GoldDust, which involved 17 countries, Europol, Eurojust and INTERPOL. All these arrests follow the joint international law enforcement efforts of identification, wiretapping and seizure of some of the infrastructure used by Sodinokibi/REvil ransomware family." READ MORE

RELATED ARTICLES:

INTERPOL, Joint global ransomware operation sees arrests and criminal network dismantled, 8 Nov 2021

Krebs on Security, REvil Ransom Arrest, $6M Seizure, and $10M Reward, 8 Nov 2021

Source: Interpol

Date: 5 Nov 2021

INTERPOL-led operation takes down prolific cybercrime ring

"A 30-month transcontinental investigation and operation has resulted in arrests and Red Notices for suspects believed to be behind a global malware crime network. […] The suspects are thought to have facilitated the transfer and cash-out of assets on behalf of the ransomware group whilst also threatening to make sensitive data public if additional payments were not made.[…] The six suspects are believed to be tightly linked to a Russian-language cybercriminal gang known for naming-and-shaming its victims on a Tor leak site, and for moving more than USD 500 million in funds linked to multiple ransomware activities." READ MORE

Source: Interpol

Date: 11 Nov 2021

Innovation to beat cybercrime acceleration the theme of 2021 Europol-INTERPOL Cybercrime Conference

"Discussions provided insight on operational highlights in tackling key cyber threats such as the astronomical growth of ransomware threats, and how new developments in technology being exploited by criminals can also be used to benefit police. "Cybercrime is an urgent global security risk, costing trillions of dollars each year. To address what is a parallel crime pandemic, law enforcement and the private sector need to take strong, collective action," said INTERPOL Secretary General Jürgen Stock." READ MORE

Source: Eurojust

Date: 8 Nov 2021

Ransomware gang dismantled with Eurojust support

"Starting in early 2019, the IT infrastructure of a significant number of companies and institutions in France, Germany and Romania was compromised by malware, rendering their data inaccessible unless the victims paid a ransom in cryptocurrencies to decrypt the compromised data. According to the investigators, the suspects were part of an international crime group behind the attacks, operating with Ransomware as a Service (RaaS)." READ MORE

Source: Council of Europe

Date: 3 Nov 2021

GLACY+: International Network of National Judicial Trainers: A new series of practitioners-to-practitioners' workshops – First workshop

"On 3 November, around 50 practitioners from 13 countries (Algeria, Azerbaijan, Brazil, Chile, Colombia, Dominican Republic, Lebanon, Mauritius, Paraguay, Senegal, Sri Lanka, Tunisia, Ukraine) participated in the first workshop of the new series of practitioners-to-practitioners workshops, organized under the framework of the International Network of Judicial Trainers. […] For this edition, three national judicial trainers from Mauritius, Senegal and Chile presented their national perspectives, allowing for various comparative analyses between different judicial systems and exchanges of views with their peers." READ MORE

Source: CENTR

Date: 8 Nov 2021

ICANN72: We need to talk about data accuracy

"[…] The question of data accuracy is now a political question, as the EU is currently negotiating the revision of its cybersecurity rules that also include a very specific point on ensuring the accuracy of registration data. This obligation is a direct consequence of the alleged impact of the GDPR on the public availability of domain name registration data within gTLDs. […] The discussions on accuracy can no longer be distinguished from the questions of who shall receive access to non-public personal information of domain name holders and when. While the EU is in the process of obliging TLDs to give it out to all "legitimate access seekers", the ICANN community is still discussing the possibility of establishing a System for Standardized Access/Disclosure (SSAD) to "centrally handle requests for non-public registration data"." READ MORE

Source: ZDnet

Date: 12 Nov 2021

Les Etats-Unis rejoignent l'appel de Paris sur la cybersécurité

"La vice-présidente des Etats-Unis, Kamala Harris, a annoncé que les Etats-Unis allaient adhérer à l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, un accord regroupant plus de 80 pays, collectivités locales et entreprises technologiques visant à promouvoir la cybersécurité et à « préserver un internet ouvert, interopérable, sûr et fiable. […] L'Appel de Paris est composé de neuf principes, qui comprennent la protection des individus et des infrastructures, la protection de l'internet, la défense des processus électoraux, la défense de la propriété intellectuelle, la non-prolifération des logiciels malveillants, la sécurité du cycle de vie, l'hygiène informatique, l'interdiction pour les acteurs privés d'avoir recours au "hack back" (ripostes aux attaques informatiques) et la mise en œuvre de normes internationales « de comportement responsable.'' READ MORE

Source: El Dinamo (Chile)

Date: 2 Nov 2021

Chile: El Sistema Nacional de Ciberseguridad: tarea digital pendiente

"Chile sigue en posiciones bajas al compararnos con los países desarrollados y, en gran parte, esto se debe a que no tenemos un marco legislativo actualizado al respecto y seguimos con leyes promulgadas cuando los computadores no estaban conectados globalmente y las redes sociales eran ciencia ficción. Es por este motivo que tenemos que aprobar muy pronto el Congreso la nueva Ley de Delitos Informáticos que contiene lo señalado en el Convenio de Budapest, del cual Chile es signatario, para poder perseguir el cibercrimen no solo en nuestro territorio, sino que a nivel transnacional." READ MORE

Source: Diario judicial

Date: 4 Nov 2021

Delitos en entornos digitales: los desafíos de la Justicia

"Según datos aportados por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECi), durante el 2020 se registraron un 565% más denuncias; los fraudes en línea crecieron más del 665% , el hackeo con softwares de ransomware 380% y corresponden a la difusión no autorizada de imágenes íntimas, 373%. […] Durante el evento se resaltó la necesidad de cooperación internacional para aplicar una política penal común, encaminada a la protección de la sociedad contra el cibercrimen. Los expertos reconocieron la importancia de la reciente incorporación de varios países de América Latina, entre ellos la Argentina, a la Convención de Budapest, donde Europa hace punta." READ MORE

Source: Krebsonsecurity

Date: 2 Nov 2021

US: The 'Groove' Ransomware Gang Was a Hoax

"A number of publications in September warned about the emergence of "Groove," a new ransomware group that called on competing extortion gangs to unite in attacking U.S. government interests online. It now appears that Groove was all a big hoax designed to toy with security firms and journalists. […] A number of publications in September warned about the emergence of "Groove," a new ransomware group that called on competing extortion gangs to unite in attacking U.S. government interests online. It now appears that Groove was all a big hoax designed to toy with security firms and journalists." READ MORE

Source: EU NEIGHBOURS

Date: 10 Nov 2021

Third meeting of the CyberSouth Judicial Network

"The third meeting of the CyberSouth Judicial Network was organised online on 9 November 2021, aiming to continue to consolidate the establishment of the Network in the region, assess the progress since the second meeting, from November 2020, and set up further objectives. The participants had the opportunity to strengthen their knowledge on international cooperation in cybercrime investigations and on the technical aspects pertaining to digital evidence and also to learn about the benefits of the International Network of the National Judicial Trainers, which enables judges and prosecutors to connect, share experience and stay informed on the latest developments in their area of expertise." READ MORE

RELATED ARTICLE:

Council of Europe, CyberSouth: Third meeting of the CyberSouth Judicial Network, 9 Nov 2021

Source: Le journal Africa

Date: 8 Nov 2021

Cybersécurité : la RDC est-elle sécurisée ?

"Internet Society Chapitre de la RD Congo et l'Institut de cybersécurité et de sécurité des infrastructures, ont organisé ce 6 novembre une masterclass sur la cybersécurité à Kinshasa. Celle-ci avec pour objectif de mener les acteurs du domaine de l'accès à internet, de la sécurité du réseau et les étudiants à approfondir leurs acquis sur la cybersécurité en RDC. [...] En 2014 à Malabo en Guinée équatoriale, les pays membres de l'Union africaine ont adopté une convention sur la cybersécurité et la protection des données à caractère personnel. Plusieurs pays ont déjà ratifié cette convention. La République Démocratique du Congo n'a pas encore adhéré au traité de Budapest ni ratifié la convention de Malabo. Ce qui rend difficile la collaboration avec certains pays en cas de cyberattaques voire contrôler ses données hébergées à l'extérieur de son territoire." READ MORE

Source: News.fr

Date: 2 Nov 2021

Le Ghana se classe 3ème en cybersécurité en Afrique

"Le niveau de développement ou d'engagement de chaque pays est évalué selon les cinq piliers stratégiques du programme mondial de cybersécurité de l'UIT (GCA) – juridique, technique, organisationnel, renforcement des capacités et coopération internationale. Un autre domaine dans lequel le pays s'est engagé dans la lutte contre la cybercriminalité a été le déploiement de points de contact pour le signalement des incidents de cybercriminalité (PoC) pour permettre aux individus et aux organisations de signaler facilement les incidents liés à la cybercriminalité." READ MORE

Source: Council of Europe

Date: 2 Nov 2021

National workshop on developing the cybercrime reporting mechanism in Algeria

"With the national workshop delivered for Algerian stakeholders, on 2nd of November 2021, the CyberSouth project, a joint action of the European Union and the Council of Europe, finalised the series of online national workshops on developing the cybercrime reporting mechanism in the priority countries. The national workshop aimed at strengthening the Algerian cybercrime reporting mechanism, through identifying new ways of collecting and processing cybercrime reports, and written practices to be followed by first responders to cybercrime investigations. The workshop was complemented by a detailed presentation delivered by the Algerian representatives of the cybercrime reporting mechanism in place and newest developments in this area." READ MORE

Source: Digital Strategy

Date: 3 Nov 2021

EU strengthens Indo-Pacific cybersecurity cooperation with week-long expert training

"The cybersecurity training was for experts from partner countries in the Indo-Pacific region and took place from 25 October to 29 October. The training is a good example of actions foreseen under the EU's new Indo Pacific Strategy, whereby the EU will intensify its dialogues with partners on security and defence, including cybersecurity, to strengthen capacity-building for partners to tackle cybercrime. [...] Japan and the EU are close partners in promoting the most advanced cybersecurity practices to other countries. First launched as a bilateral exercise between Japan and the United States in 2018, the EU has now been involved since 2020, becoming a formal partner this year." READ MORE

Source: The Newsmen

Date: 6 Nov 2021

Collecting electronic evidence to prevent attacks posing challenge to agencies: UNSC

"The exponential rise in using the Internet and social media by terrorists in South Asia including India has been a challenge to the Law Enforcing Agencies (LEA) to prevent terror attacks and bringing terrorists and other criminals to justice, the United Nations Security Council flags in its latest report. According to the report, the officials investigating, and prosecuting terrorism, organized crime and other serious criminal cases regularly confront the challenge of how to obtain electronic evidence in trying to prevent attacks and in bringing terrorists and other criminals to justice." READ MORE

Source: Perth now

Date: 12 Nov 2021

Austrialia: Electronic items, digital evidence seized as alleged child abuse offenders caught up in police sting

"A police operation targeting the possession and distribution of child exploitation material led to a number of Queensland men being charged with child abuse offences. During the five-day operation, a number of electronic items and digital evidence was seized from various homes on the Sunshine Coast. After officers searched a 30-year-old Sunshine Coast man's home, he was charged with 43 child abuse related offences." READ MORE

Source: Le Figaro

Date: 12 Nov 2021

Un groupe de cybercriminels russophones a ciblé plus de 3500 particuliers et entreprises en 18 mois

"Avec plus de 3500 cibles en 18 mois, le groupe de cybermercenaires Void Balaur s'est imposé comme une référence dans le monde de la cybercriminalité et du cyberespionnage […] Ce cyberespionnage cible également des acteurs stratégiques à travers le monde. L'une des campagnes les plus importantes de ces pirates aurait ciblé les adresses mail privées de cinq ministres et deux membres du parlement d'un pays d'Europe de l'Est. Ils ont aussi récemment ciblé des personnalités politiques au Kazakhstan, en Ukraine, en Slovaquie, en Russie en Norvège, en Arménie en Italie ou encore en France, affirme le rapport." READ MORE

Source: Info security magazine

Date: 5 Nov 2021

UK: ONS Reports Huge Spike in Cybercrime and Fraud During COVID-19

"Published by the Office for National Statistics (ONS), the figures further demonstrated the extent to which crime shifted to the digital space during COVID-19 lockdown restrictions in the UK. There was an estimated 14% decline in total crime excluding computer misuse and fraud in 2020/21 compared with 2018/19. […] There was also an estimated 32% rise in fraud cases, according to the TCSEW. This appeared to be largely driven by substantial increases in "consumer and retail fraud" and "advance fee fraud." This indicates that fraudsters have adapted to new behaviors such as the shift to online shopping and banking during the pandemic." READ MORE

Latest reports

- Sophos, Interrelated threats target an interdependent world, November 2021
- GlobalsecurityMag, Le rapport Zscaler 2021 sur les attaques chiffrées, November 2021
- Confédération suisse, Deuxième rapport semestriel du NCSC: gros plan sur les vulnérabilités, 2 November 2021
- Intel 471, Cybercrime underground flush with shipping companies' credentials, 2 November 2021
- Infosecurity, Annual Cost of Child Identity Fraud Almost $1Bn, 2 November 2021
- Javelin Strategy, Child Identity Fraud: A Web of Deception and Loss, 2 November 2021
- Cloudfare, DDoS Attack Trends for Q3 2021, 4 November 2021
- CERT-FR, Rapport menaces et incidents du CERT-FR, 4 November 2021
- Brill, The Potential and the Challenges of Digital Evidence in International Criminal Proceedings, 9 November 2021
- Trend Micro, The Far-Reaching Attacks of the Void Balaur Cybermercenary Group, 10 November 2021
- Conflictoflaws, How Emerging Technologies Shape the Face of Chinese Courts?, 10 November 2021
- EUROPOL, IOCTA 2021 unveils the most recent cyber threat (r)evolutions, 11 November 2021
- ENISA, CSIRT Capabilities in Healthcare Sector, 11 November 2021
- Europol, INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2021, 11 November 2021
- Derecho penal online, El delito de grooming y su investigación a la luz del Código Procesal Penal de Mendoza, 11 November 2021
- Threatpost, Top 10 Cybersecurity Best Practices to Combat Ransomware, 12 November 2021
- IACP Cyber Center, Handling evidence from specific sources
- Insurance Information Insititute, Facts + Statistics: Identity theft and cybercrime

Upcoming events

- 16-18 November, C-PROC, (*online/hybrid*), OCTOPUS Conference 2021, 20th Anniversary of the Budapest Convention, OCTOPUS,
- 16-18 November, C-PROC/CARICOM IMPACS, Series of trainings for law enforcement: electronic evidence session, OCTOPUS,
- 22-25 November, C-PROC/TUNISIA, *(hybrid)*, Training of Trainers workshop on cybercrime and e-evidence for Tunisian magistrates, CyberSouth
- 23-25 November, C-PROC/NORTH MACEDONIA, *(online),* Domestic/online practical exercise bringing together cybercrime, cybersecurity and the private sector aimed at developing practical skills of public-private co-operation, iPROCEEDS-2
- 23-25 November, C-PROC/CARICOM IMPACS, Series of trainings for law enforcement: SOPs and financial investigation session, OCTOPUS,
- 24 November, C-PROC, (*online*), Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime, GLACY+, CyberSouth, iPROCEEDS-2, OCTOPUS,
- 24 November, C-PROC/AZERBAIJAN, *(in person)*, Supporting TOPCOP project training on cryptocurrencies and darkweb for Azerbaijani investigators, CyberEast
- 26 November, C-PROC/PILON, (*online*), Regional Workshop on cybercrime: 'Countering Disinformation' Webinar, GLACY+
- 26-27 November, C-PROC/IAWJ, (*online*), Regional conference on cybercrime for women judges in LATAM and CARIBBEAN region, OCTOPUS, GLACY+
- 29 November - 2 December, C-PROC/JORDAN, *(in-person),* Training of Trainers workshop on cybercrime and e-evidence for Jordanian magistrates, CyberSouth
- By 29 November (TBC), C-PROC/ECUADOR, (*online*), Desk review of the Data Protection secondary legislation, in collaboration with the Data Protection Unit of the Council of Europe, GLACY+
- 30 November - 2 December, C-PROC/CARICOM IMPACS, Series of trainings for law enforcement: international cooperation and MLA, OCTOPUS,

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