# Cybercrime Digest

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

1-15 August 2018

*Source: Europol*

*Date: 2 Aug 2018*

## Over 2 million pieces of child abuse material seized in Spain, with the support of Europol and INTERPOL

"The Spanish National Police with the support of Europol and INTERPOL arrested 19 members of one of the biggest child abuse networks in Spain. The gang, operating across Europe and America, used 14 different groups in an instant messaging service to share the illicit content. The individuals hide their identities by using specific anonymisation software. On the action day, 19 house searches were carried out in several Spanish cities, and police officers seized 11 laptops, 23 mobile phones, 4 tablets, 11 hard drive disks, 7 memory sticks and 5 memory cards. The investigation revealed that all of these devices - 16 terabytes in total, contained some 2 400 000 pieces of footage of children between the age of 0 and 8 years old being abused. Due to the network which operated in different countries, making it an international cross-border case, Europol supported the Spanish authorities by facilitating the information exchange and crosschecking the data contributed by Spain. These images and videos were processed for victim identification." READ MORE

RELATED ARTICLES

INTERPOL, Child abuse victims rescued in Spanish operation, 7 Aug 2018

---

*Source: The Register*

*Date: 7 Aug 2018*

## ICANN loses a third time in WHOIS/ GDPR legal war

"EPAG wanted to sell domain names without collecting the domain owners' administrative and technical contact details because it feared doing so would put it at risk of ruinous fines if it ran afoul of GDPR. […] To force it to comply with its registrar contract, ICANN took EPAG to court in May, seeking an order banning the registrar from peddling domain names if it refused to gather data for Whois. The row eventually reached Cologne's appeals court, which this month declared it found the two previous rulings against ICANN "convincing," and noted that there was "no imminent emergency" that justified a request for an emergency injunction. […] The court also rejected ICANN's insistence that the matter be sent to the European Court of Justice, noting that it was "under no obligation to refer the case to the ECJ" because ICANN's interpretation of the law "was not material to the decision."." READ MORE

---

*Source: IDG Connect*

*Date: 6 Aug 2018*

## GDPR-based extortion, the next cybercrime trend

"GDPR came into force on 25th May 2018. […] Now that the regulations have come into force […] a number of companies have predicted that the regulations could lead to a rise in cyber-extortion; criminals breaching a company or discovering they are not GDPR complaint – and demanding money in return for not reporting them to the Information Commissioner's Officer or equivalent data regulator. […] Moreover, the GDPR legalization gives individuals and groups the right to compensation for infringement, and experts predict criminals could threaten a company with class action from multiple consumers who have been impacted by a GDPR failure." READ MORE

*Source: Council of Europe*

*Date: 3 Aug 2018*

## Special Programme on Cybercrime for the Supreme Court Justices of Mauritius

"The Council of Europe organized a dedicated high level workshop on cybercrime and electronic evidence for the Supreme Court Justices of Mauritius. A large majority of the Supreme Court Judges were actively engaged over the three-day program. The content was specifically crafted on the needs expressed by the Mauritian judiciary during the initial assessment, and included practical sessions with case studies to stimulate debate on how to effectively apply the law and what are the opportunities offered to Mauritius as a Party to the Budapest Convention. A follow up will be planned in the spring of 2019, so as to build upon the competencies already acquired by the Supreme Court Justices and to consolidate the role of Mauritius as a judicial training hub for the Southern African Development Community (SADC) region on matters related to cybercrime and electronic evidence. " READ MORE

*Source: Niamey et le 2 jours*

*Date: 3 Aug 2018*

## Le Niger va adhérer à la Convention sur la cybercriminalité qui vise la mise en place d'une politique pénale contre la criminalité via internet

"Le gouvernement en conseil des ministres le 1er août dernier, a adopté un projet d'ordonnance autorisant l'adhésion du Niger à la Convention sur la cybercriminalité, signée le 20 janvier 2003 à Strasbourg entre les Etats membres du Conseil de l'Europe et d'autres Etats signataires. Ladite convention est un instrument juridique qui vise la réalisation de plusieurs objectifs dont l'adoption d'une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, à travers une législation appropriée et par l'amélioration de la coopération internationale ; la lutte contre le risque de l'utilisation des réseaux informatiques et de l'information électronique pour commettre des infractions pénales ; la création d'un cadre de lutte contre la cybercriminalité à l'échelle internationale en matière pénale et enfin, la coopération entre les Etats et l'industrie privée. D'après le Conseil européen, cette convention est le premier instrument conventionnel contraignant, spécifiquement élaboré, pour lutter contre la cybercriminalité et toutes les infractions pénales commises à travers Internet et d'autres réseaux informatiques." READ MORE

*Source: Vanguard*

*Date: 8 Aug 2018*

## Ghana police arrest 12 suspects in the biggest cyber-crime operation in Ghana

"The Criminal Investigation Department of the Ghana Police Service have arrested 12 suspected criminals in the biggest ever cyber-crime in recent times in the country. An Accra Circuit Court on last Friday remanded into police custody 11 out of the 12 suspected bank fraudsters. The court also ordered the suspects to reappear on August 9, 2018 to assist police conduct further investigations into the financial crime. According to the police, all the suspects, believed to be part of a wider cyber-crime syndicate made up of Nigerians and Ghanaians, attempted transferring a whopping GHC326 million from the vault of Universal Merchant Bank, electronically. […] After detecting the security breaches the bank alerted the Financial Forensics Unit of the CID, who dispatched personnel to all branches of the bank to arrest persons who will visit the branches to withdraw money from some identified accounts." READ MORE

*Source: Emirates News Agency*

*Date: 13 Aug 2018*

## UAE Cybercrimes Law amended, introducing greater punishments for terrorism-related offences

"President His Highness Sheikh Khalifa bin Zayed Al Nahyan issued Emiri Decree No. 02 of 2018 amending the UAE Cybercrimes Law. According to the Decree, Article Nos. 26, 28 and 42 of Federal Decree-Law No. 05 of 2012 on Combatting Cybercrimes will be replaced with updated provisions. Article No. 26 stipulates an imprisonment period of at least ten years and not exceeding 25 years, and a fine not less than AED2 million and not in excess of AED4 million on whoever establishes, manages or runs a website or publishes information on the computer network or information technology means for the interest of a terrorist group or any unauthorised group, association, organisation, or body with the intent to facilitate communication with their leaders or members or attract new members, or to promote or praise their ideas, finance their activities or provide actual assistance thereof or for the purpose of publishing methods for manufacturing incendiary devices or explosives or any other devices used in terrorism acts." READ MORE

*Source: South China Morning Post*

*Date: 10 Aug 2018*

## Hong Kong cybercrime law must not be a catch-all that compromises police

"The offence that criminalises "access to a computer with dishonest or criminal intent" has been the subject of debate in Hong Kong for years. From taking upskirt photos to leaking exam papers; from cyber frauds and hacking to leaving provocative comments on the internet, the charge has been increasingly used in a wide range of cases. While critics see it as too sweeping and arbitrary, officials say it is an effective tool in combating crime. Introduced amid growing concerns over cybercrime in 1993, the offence imposes a maximum of five years in jail on anyone obtaining access to a computer with the intent to commit an offence, a dishonest intent to deceive, a view to dishonest gain for oneself or another, or to cause losses to another. Of the 293 cases prosecuted between 2008 and 2014, 252 resulted in convictions, representing a rate of more than 85 per cent. Powerful as it, the law is being used in an array of cases, so much so that critics say it may be used arbitrarily." READ MORE

*Source: 9News*

*Date: 14 Aug 2018*

## Tougher planned cybercrime laws target tech giants in Australia

"Law enforcement agencies will gain the power to read messages on games such as Call of Duty and Fortnite under tough planned new cyber security laws. The Turnbull government is set to unveil legislation which would force technology companies to disclose encrypted information on devices and social media platforms. Technology companies and civil libertarians have warned the changes would weaken privacy protections, but Cyber Security Minister Angus Taylor says law enforcement agencies need the new powers. He said technologies including encryption are increasingly being used by paedophiles, terrorists and organised criminals to conceal their illicit activities. "We know that more than 90 per cent of data lawfully intercepted by the Australian Federal Police now uses some form of encryption. "This has directly impacted around 200 serious criminal and terrorism-related investigations in the last 12 months alone," Mr Taylor said." READ MORE

*Source: CIO Mag*

*Date: 5 Aug 2018*

## L'Afrique se met en ordre de bataille contre la cybermalveillance et la cybercriminalité

"Depuis l'adoption il y a quatre ans de la Convention de Malabo sur la cybersécurité, une toute petite minorité d'Etats africains l'ont ratifiée. Or la seule souveraineté numérique d'un pays ne suffira pas à le protéger contre les cyberattaques qui, en 2017, ont fait perdre au Continent 3,5 milliards de dollars. Et le fléau n'ira qu'en empirant si la défense ne s'organise pas mieux." READ MORE

*Source: Agence d'Information d'Afrique Centrale*

*Date: 8 Aug 2018*

## Economie numérique : la cyber législation congolaise passée au peigne fin

"Des délégués et experts de plusieurs institutions du pays ont examiné et amendé, le 8 août à Brazzaville, les avant-projets de loi réglementant le secteur, dans la perspective de leur prochaine adoption par le gouvernement. L'atelier organisé et piloté par le ministère des Postes, des télécommunications et de l'économie numérique a été l'occasion de présenter les nouvelles moutures des projets de textes sur l'économie numérique et placer tous les acteurs impliqués au même niveau d'information, dans le respect de la transversalité et le dynamisme de ce secteur. Rehaussé de la présence du ministre de tutelle, Léon Juste Ibombo, et de son homologue de la Recherche scientifique et de l'innovation technologique, Parfait Aimé Coussoud Mavoungou, le rendez-vous a permis d'examiner tant sur le fond que sur la forme ces textes qui ont déjà reçu l'approbation de la Cour suprême." READ MORE

*Source: Derechos Digitales*

*Date: 9 Aug 2018*

## La necesidad de legislar sobre cibercrimen en Panamá

"Una reforma adecuada permitiría que los mecanismos para la investigación penal aseguren la correcta guía y salvaguarda de los derechos humanos y garantías procesales reconocidos por tratados internacionales y la Constitución. […] La Asamblea Nacional de Panamá aprobó el Convenio sobre la Ciberdelincuencia a través de la Ley 79 del 22 de octubre de 2013. […] Sin embargo, actualmente, el Código Penal vigente únicamente tipifica 2 conductas como delitos informáticos, y no incluye los delitos que se realicen por medios electrónicos. […] En ese sentido, Panamá tiene la obligación internacional de adecuar su legislación penal conforme a los estándares regulados en el Convenio de Budapest, lo que implica elaborar reformas al Código Penal y Código Procesal Penal." READ MORE

*Source: The Nation*

*Date: 14 Aug 2018*

## Sophisticated cybercrime on the rise in Vietnam

"As reliance on information technology becomes ever more pervasive in society, cybercrime has grown rapidly both in quantity and sophistication in Vietnam, experts said. The Ministry of Public Security has recently worked with police departments in 52 provinces and cities to dismantle cases of fraud through the use of the Internet, telecommunications and banking system to illegally appropriate property. […] Some believe the Law on Cybersecurity recently adopted by the National Assembly and taking effect in January 1 will be an effective tool to protect the online community and to assist in the fight against hi-tech cybercrime. […] According to the Ministry of Public Security, once the law is implemented, it will help protect users from malicious information that could affect their honour, reputation and dignity." READ MORE

*Source: BBC*

*Date: 15 Aug 2018*

## Taner Kilic: Amnesty Turkish chair to be released from prison

"Turkey has decided to release the national head of Amnesty International after more than a year in prison. […] Mr Kilic was arrested in June 2017 along with 22 lawyers, accused of using an encrypted messaging app called Bylock, which the Turkish government said was used by members of the banned group. Amnesty said Mr Kilic had never downloaded the app, and had not even heard of it until its existence was widely reported in the mainstream press. The following month, the director of Amnesty in Turkey, Idil Eser, was also arrested in Istanbul alongside nine others. They were released on bail months later, but are still facing charges of membership of a terrorist organisation." READ MORE

RELATED ARTICLES

Turkish Minute, 38 people warranted over ByLock use and Gülen links, 14 Aug 2018

*Source: Action Fraud UK*

*Date: 10 Aug 2018*

## UK, Cryptocurrency fraud leads to £2 million worth of losses this summer

"Fraudsters are cold calling victims and using social media platforms to advertise 'get rich quick' investments in mining and trading in cryptocurrencies. Fraudsters will convince victims to sign up to cryptocurrency investment websites and to part with their personal details such as credit card details and driving licences to open a trading account. The victim will then make an initial minimum deposit, after which the fraudster will call them to persuade them to invest again in order to achieve a greater profit. In some cases, victims have realised that they have been defrauded, but only after the website has been deactivated and the suspects can no longer be contacted. Between 1 June 2018 and 31 July 2018, 203 reports of fraud involving cryptocurrency were reported. The total reported loss was £2,059,501.29." READ MORE

## Latest reports

- Council of Europe, GLACY+: 2018/AO/45 - Call for tenders - 31 August 2018 - Provision of event organisation services in Addis Ababa, Ethiopia, published on 31 Jul 2018
- Anti-Phishing Working Group, Phishing Activity Trends Report 1Q2018, 31 Jul 2018
- Lusthaus, Is the Mafia taking over Cybercrime?, Black Hat USA Conference, 4 Aug 2018
- Juniper Research, Cybersecurity Breaches to Result in Over 146 Billion Records Being Stolen by 2023, 8 Aug 2018
- Malwarebytes, Cybercrime tactics and techniques: Q2 2018, Aug 2018

# Upcoming events

- 20-24 August, Nuku'alofa, Tonga – ECTEG Course on Open-Source forensics and Mobile forensics, GLACY+
- 20-24 August, Port Vila, Vanuatu – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, GLACY+
- 27 August, Tunis, Tunisia – Advisory mission on 24/7 contact point, CyberSouth
- 27-30 August, Nuku'alofa, Tonga – Advanced Judicial Training on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers with participation of countries from the Pacific Region, GLACY+
- 27-31 August, Singapore – Joint International Workshop for Cybercrime Investigation Units and MLA Central Authorities, GLACY+
- 29-30 August, Beirut, Lebanon – Advisory mission on setting up a CSIRT, CyberSouth
- 30 August, Nuku'alofa, Tonga – In-country advisory mission on integration/ mainstreaming of training modules in curricula of training institutions, GLACY+
- 31 August, New Delhi, India – ASSOCHAM Annual meeting 2018, Cybercrime@Octopus



COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

**www.coe.int/cybercrime**