Cybercrime Digest

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

16-30 April 2018

Source: European Commission

Date: 17 Apr 2018

Security Union: European Commission facilitates access to electronic evidence

"The European Commission is proposing new rules to make it easier and faster for police and judicial authorities to obtain the electronic evidence, such as e-mails or documents located on the cloud, they need to investigate, prosecute and convict criminals and terrorists. The new rules will allow law enforcement in EU Member States to better track down leads online and across borders, while providing sufficient safeguards for the rights and freedoms of all concerned. […] Criminals and terrorists all use text messages, emails and apps to communicate. More than half of all criminal investigations today include a cross-border request to obtain electronic evidence held by service providers based in another State. To obtain such data, judicial cooperation and mutual legal assistance is needed, however, the process is much too slow and cumbersome at present. Today, almost two thirds of crimes where electronic evidence is held in another country cannot be properly investigated or prosecuted, mainly due to the time it takes to gather such evidence or due to fragmentation of the legal framework. By making the process of obtaining electronic evidence more quickly and efficiently, proposals will help close this loophole. […] The proposals will: (i) create a European Production Order; (ii) prevent data being from being deleted with a European Preservation Order; (iii) include strong safeguards and remedies; (iv) oblige service providers to designate a legal representative in the Union; (v) provide legal certainty for businesses and service providers." READ MORE

Source: The Guardian

Date: 27 Apr 2018

Joint police action 'punches big hole' in Isis propaganda ability

"Law enforcement authorities have "punched a big hole" in Islamic State's propaganda machine, targeting news agencies and radio stations used by the jihadi group to radicalise people across the world. Isis computer servers in the Netherlands, Canada and the US, as well as digital evidence in Bulgaria, France and Romania, have been seized in a two-day takedown operation co-ordinated by Europol. The action targeted Isis-branded media outlets such as Amaq and Nashir news agencies and al-Bayan radio, hitting the extremist organisation's ability to broadcast and publicise terrorist material." READ MORE

Source: Poder Judicial Republica de Chile

Date: 19 Apr 2018

Chile, Presidente de la Corte Suprema se reúne con expertos del proyecto contra delitos cibernéticos

"El presidente de la Corte Suprema (S) Hugo Dolmestch sostuvo ayer –miércoles 18 de abril- una reunión con el equipo de expertos que desarrollan el proyecto Acción Global contra los delitos cibernético (GLACY +, por sus siglas en inglés) lanzado por el Consejo de Europa y la Comisión Europea. La visita se enmarca en una misión de evaluación inicial que tiene por objeto apoyar a Chile en la aplicación del Convenio de Budapest, ratificado en abril de 2017." READ MORE

Nigerian government taking steps to fight cyber crime

"The Federal Government has taken several steps through domestic policies and legislation, as well as multilateral cooperation and collaboration to fight cybercrime, the Attorney-General of the Federation, (AGF), Abubakar Malami, said. Mr Malami said this on Tuesday in Abuja at a meeting with a delegation of the Council of Europe on an Initial Assessment Visit to Nigeria and inauguration of the Global Action on Cyber Crime Plus, (GLACY+), National Coordinating Team. […] The AGF who doubles as the Minister of Justice noted that in spite of the country's efforts, there were still gaps in capacity building considering the fast evolving technological developments. "It is in this light that we welcome this initial assessment visit to identify the priorities that criminal justice authorities in Nigeria have to face, to pinpoint which areas to cover through the capacity building action of the GLACY+ Project." READ MORE

RELATED ARTICLES

Technology Times, Nigeria looks beyond border in cybercrime push, 25 Apr 2018

Face à la cybercriminalité, l'Afrique de l'Ouest s'organise sous la pression et avec l'aide de la France

"En Côte d'Ivoire comme au Bénin, les cybercriminels prospèrent grâce à des escroqueries qui font des victimes jusqu'en France. Face à l'ampleur du phénomène, des États africains s'outillent juridiquement pour mieux les combattre. […] La France accompagne des pays africains sur le plan de la formation des policiers et les dote d'équipements. Au Bénin, un laboratoire financé par Paris permet de remonter à des preuves cachées au sein d'un ordinateur ou d'un portable perquisitionné. La Côte d'Ivoire dispose pour sa part d'un centre de surveillance du cyberespace en temps réel." READ MORE

Facebook, YouTube release data on extremist content removal

"Facebook removed or added warnings to 1.9 million pieces of content related to terror groups Islamic State and al-Qaeda in the first quarter of 2018, close to double the number it removed the previous quarter, it said in a statement released overnight. The number is likely lower than the total volume of content removed, as Facebook also removes profiles, pages and groups that violate community standards and does not go through that content to label it as terrorism-related after it has been taken down, it said. The social media platform has beefed up its counterterrorism team to 200 people from 150 last June and built specialized techniques to find and remove old content, according to its statement. In 99 percent of cases, the content taken down was detected by internal reviewers, not reported by users." READ MORE

Ransomware infects Ukraine energy ministry website

"Hackers have used ransomware to take the website of Ukraine's energy ministry offline and encrypt its files. The website currently contains a message written in English, demanding a ransom of 0.1 bitcoin - worth $927.86 (£664.98) by today's exchange rate. Ukranian cyber-police spokeswoman Yulia Kvitko said the attack is an "isolated incident" and no other government websites have been affected." READ MORE

Source: The Register

Date: 27 Apr 2018

Europe fires back at ICANN's plan to overhaul Whois for GDPR by next year

"On March 26 – two months before new privacy protections come into effect in Europe – Goran Marby, CEO of DNS overlord ICANN, sent a letter [PDF] to each of Europe's 28 data protection authorities (DPAs) asking them to hold off punishing it over Whois. […] That open-ended moratorium became fixed: a one-year extension for ICANN to introduce its new system. ICANN then solicited input from other groups – including the US government – to back up its idea and took a series of letters along with a proposed timeline showing a one-year moratorium to a meeting of the Article 29 Working Party (WP29) in Brussels. […] There was however a big problem with this whole effort: there can be no such thing as a moratorium on regulations that are already in place. In a new statement, provided by the Article 29 Working Party to The Register on Thursday following its meeting with ICANN earlier this week, the group is clearly baffled by ICANN's repeated requests for something that doesn't exist. "The GDPR does not allow national supervisory authorities nor the European Data Protection Board to create an 'enforcement moratorium' for individual data controllers," the statement notes. "Data protection is a fundamental right of individuals, who may submit complaints to their national data protection authority whenever they consider that their rights under the GDPR have been violated."." READ MORE

Source: Egypt Today

Date: 17 Apr 2018

Egypt, Parliamentary committee approves draft cybercrime law

"Parliament's Communications and Information Technology Committee approved the draft cybercrime law on Monday, which aims to pose surveillance on social media and limit the spread of fake news, particularly those that incite violence. […] If a website published content that violates the cybercrime law, then those responsible for the violation would be judged and the website would be banned if the violation was repeated. […] On Wednesday, the Cabinet referred the draft cybercrime law to Parliament to be discussed, as the law has an indispensable role in dealing with rumors that are not easily monitored on social media. The punishments set forth in the draft law range from a month in prison to the death penalty, should, in the latter case, the cybercrime result in the death of someone or is considered a threat to national security." READ MORE

Source: Marca Sur

Date: 18 Apr 2018

Argentina will make changes in the Criminal Code to combat piracy

"In 2018 the Argentinian government will move towards a modification of the Criminal Code, incorporating crimes against IP concerning copyright, trademarks and patents. New criminal types will be incorporated, mainly by the implementation of the WIPO treaties of 1996 and the Budapest Convention on cybercrimes", the Director of the National Directorate of Copyright informed. The WIPO Copyright Treaty is a special agreement under the Berne Convention which deals with the protection of works and the rights of their authors in the digital environment, while the Budapest Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security." READ MORE

Source: Europol

Date: 25 Apr 2018

World's biggest marketplace selling internet paralysing DDoS attacks taken down

"The administrators of the DDoS marketplace webstresser.org were arrested on 24 April 2018 as a result of Operation Power Off, a complex investigation led by the Dutch Police and the UK's National Crime Agency with the support of Europol and a dozen law enforcement agencies from around the world. The administrators were located in the United Kingdom, Croatia, Canada and Serbia. Further measures were taken against the top users of this marketplace in the Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada and Hong Kong. The illegal service was shut down and its infrastructure seized in the Netherlands, the US and Germany. Webstresser.org was considered the world's biggest marketplace to hire DDoS services, with over 136 000 registered users and 4 million attacks measured by April 2018. The orchestrated attacks targeted critical online services offered by banks, government institutions and police forces, as well as victims in the gaming industry." READ MORE

Source: BBC

Date: 17 Apr 2018

Russia's Telegram block hits web users

"Russian web users are reporting problems accessing online services as a result of the authorities' bid to block the Telegram messaging app. Russia's media regulator has blocked more than 4 million IP addresses after a court approved its request to shut the app down. Telegram is reportedly using the addresses to get around the block. Retailers, online games and another message service - Viber - are also said to have been affected." READ MORE

Latest reports

- Council of Europe, Octopus Conference, Registration open until 10 Jun 2018, 1 May 2018
- European Commission, Proposal for a Regulation of the European Parliament and of The Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 Apr 2018
- Council of Europe, Self-Guided Training Manual: Advanced Course on the Search, Seizure and Confiscation of Online Crime Proceeds, 23 Apr 2018
- G7, Chair's report of the meeting of the G7 Ise-Shima Cyber Group, April 2018
- G7, G7 Foreign Ministers' joint communiqué, 23 Apr 2018
- European Commission for democracy through law (Venice commission), 15th European Conference of Electoral Management Bodies "Security in Elections" – Synopsis and Conclusions, 20 Apr 2018
- ENISA, Strengthening network & information security & protecting against online disinformation ("fake news"), 27 Apr 2018
- Commonwealth, Cyber Security - Capacity Buildinig in the Commonwealth, April 2018
- IETF, O'Reilly, Analysis of the Crime Attribution Characteristics of Various IPv6 Address Assignment Techniques, 24 Apr 2018

Upcoming events

- 2-4 May, Banjul, Gambia – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, GLACY+
- 3-4 May, Kyiv, Ukraine – Fourth Regional meeting on Improving international cooperation on cybercrime in the Eastern Partnership region (MLA and 24/7 working groups), Cybercrime@EAP 2018
- 5-7 May, Dakar, Senegal – Participation in AfriNIC Government Working Group (AfGWG) and ICANNs Capacity Development Workshop for African GAC members Law Enforcement and Consumer Protection Agencies, GLACY+
- 7-11 May, Dakar, Senegal – Regional Basic Law Enforcement Training of Trainers on Cybercrime and Electronic Evidence for African Officers of Gendarmerie, GLACY+
- 8-10 May, Cebu, Philippines – National Roll-out of Introductory training delivered by national prosecutors and judges trained trainers, GLACY+
- 8-10 May, Tehran, Iran – Participation in INTERPOL Eurasian Working Group on Cybercrime for Heads of Units, GLACY+
- 8-11 May, Beirut, Lebanon – Joint Advisory Mission to ISF capabilities, CyberSouth and and CT MENA
- 11 May, Rome, Italy - Lecture on the Budapest Convention within the Cybersecurity Master program, Libera Università Internazionale degli Studi Sociali Guido Carli (LUISS), GLACY+
- 8-12 May, Dublin, Ireland – Support in participation in long-distance master programme at UCD (Summer examination of participants), iPROCEEDS
- 11-13 May 2018, Vienna, Austria – T-CY Protocol Drafting Group Meeting, T-CY
- 14 May, Vienna, Austria – GLACY+ 4th Steering Committee Meeting, GLACY+
- 14-15 May, Bucharest, Romania – Regional workshop on criminal justice statistics and electronic evidence, iPROCEEDS
- 14-17 May, Rabat, Morocco – Basic Judicial Training, CyberSouth
- 14-18 May 2018, Vienna, Austria – UN Commission for Crime Prevention and Criminal Justice (UNCCPCJ), iPROCEEDS / CyberSouth / Cybercrime@EAP 2018 / GLACY+ / Cybercrime@Octopus

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime