Cybercrime Digest

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

1-15 June 2018

Source: Council of Europe

Date: 6 Jun 2018

Argentina joins the Budapest Convention

"The authorities of Argentina have deposited the instrument of accession to the Budapest Convention on Cybercrime. With this, the number of Parties of this treaty will increase to 58. A further 13 States have signed it or been invited to accede."

RELATED ARTICLES

Council of Europe, State of signatures, ratifications and accessions to the Budapest Convention on Cybercrime, 6 Jun 2018

La Vanguardia, Argentina, séptimo país americano en adherirse al Convenio sobre cibercrimen, 6 Jun 2018

Source: DN

Date: 7 Jun 2018

Peritos recomendam a Cabo Verde especialização na investigação e combate ao cibercrime

"A criação de uma unidade policial especializada, reforço da formação, alterações legislativas sobre conservação de provas digitais e sistematização de dados estatísticos são algumas das recomendações feitas a Cabo Verde no âmbito do combate à cibercriminalidade. As recomendações constam do diagnóstico feito por uma equipa de peritos do Conselho da Europa, que entre segunda-feira e hoje esteve no país para avaliar as competências em matéria de cibersegurança. A missão decorreu no âmbito do Projeto GLACY, de cuja assistência técnica Cabo Verde passará a beneficiar por ter aderido à Convenção de Budapeste, o único tratado internacional sobre cibercrime e prova digital." READ MORE

RELATED ARTICLES

Council of Europe, GLACY+: Cape Verde joins the project to build up national capacities on cybercrime, 7 Jun 2018

Source: Europol

Date: 4 Jun 2018

Masterminds behind CEO fraud ring arrested after causing more than EUR 18 million of damage

"On 28 May the French National Gendarmerie - Section de Recherches of Bordeaux, supported by the Israeli authorities and Europol, arrested the main suspects of an organised crime group behind a total of 24 cases if CEO fraud across Europe to the detriment of Belgian and French-based commercial companies, causing more than EUR 18 million worth of damage. In the framework of this large-scale CEO fraud operation, seven individuals had been already arrested in previous phases of the investigation in Belgium and France through coordinated actions, also supported by Europol. This investigation is the follow-up of systematic operational activities initiated in 2016 when two French companies fell victim to CEO fraud, incurring an estimated EUR 1.2 million financial loss. The continued investigative efforts made by the French investigators, along with the substantial information exchange and analysis, allowed them to identify and locate four individuals operating from Israel considered to be the masterminds of the busted criminal ring." READ MORE

Source: Turkish Minute

Date: 7 Jun 2018

Police cybercrime unit monitoring 45 million social media accounts in Turkey

"The Turkish National Police's anti-cybercrime department is monitoring some 45 million social media users in the country for possible criminal activity committed through the Internet. Department authorities told the Hürriyet daily that online procurement, drug trafficking and illegal betting are the most commonly committed crimes on social media platforms, followed by insulting state authorities. The department has established a special desk dedicated to insult amid a spate of cases opened in recent years for "insulting" President Recep Tayyip Erdoğan." READ MORE

RELATED ARTICLES

Turkish Minute, Detention warrants issued for 77 over ByLock use, 7 Jun 2018

Source: The New York Times

Date: 3 Jun 2018

Facebook Gave Device Makers Deep Access to Data on Users and Friends

"As Facebook sought to become the world's dominant social media service, it struck agreements allowing phone and other device makers access to vast amounts of its users' personal information. Facebook has reached data-sharing partnerships with at least 60 device makers — including Apple, Amazon, BlackBerry, Microsoft and Samsung — over the last decade, starting before Facebook apps were widely available on smartphones, company officials said. The deals allowed Facebook to expand its reach and let device makers offer customers popular features of the social network, such as messaging, "like" buttons and address books. […] Facebook allowed the device companies access to the data of users' friends without their explicit consent, even after declaring that it would no longer share such information with outsiders. Some device makers could retrieve personal information even from users' friends who believed they had barred any sharing, The New York Times found." READ MORE

The New York Times, Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence, 5 Jun 2018

Source: Georgia Today

Date: 6 Jun 2018

On EuroDIG 2018

"An annual conference "European Dialogue on Internet Governance (EuroDIG 2018)" was held on June 5-6 in Tbilisi. […] We sat down with the Head of Information Society of the Council of Europe, Patrick Penninckx, to find out more. […] "Hate speech is largely about the context, and that leaves a lot of room for interpretation. The regulatory environment that is being developed in a very specific context may be used by totalitarian or monopolistic regimes, adapted to their own purposes. They may say, 'see, they're doing this restriction on freedom of expression in Germany, they're doing it in the UK, why shouldn't we be able to do the same?' So, the states with stronger democratic traditions have to be very careful about the possible impact of their legislation on other countries, how it might be used and interpreted in a completely different context, leading to a negative effect on the plurality of opinions"." READ MORE

RELATED ARTICLES

Council of Europe, Challenges of cybercrime and transborder investigations discussed at EuroDIG 2018, 6 Jun 2018

Source: ICANN

Date: 13 Jun 2018

ICANN Appeals German Court Decision on GDPR / WHOIS

"ICANN today appealed a decision by the Regional Court in Bonn, Germany not to issue an injunction in proceedings that ICANN initiated against EPAG, a Germany-based, ICANN-accredited registrar that is part of the Tucows Group. […] ICANN is asking the Higher Regional Court of Cologne to issue an injunction that would require EPAG to reinstate the collection of all WHOIS data required under EPAG's Registrar Accreditation Agreement with ICANN. The Regional Court in Bonn rejected ICANN's initial application for an injunction, in which ICANN sought to require EPAG to collect administrative contact and technical contact data for new domain name registrations. If the Higher Regional Court does not agree with ICANN or is not clear about the scope of the European Union's General Data Protection Regulation (GDPR), ICANN is also asking the Higher Regional Court to refer the issues in ICANN's appeal to the European Court of Justice. ICANN is appealing the 30 May 2018 decision by the Regional Court in Bonn as part of ICANN's public interest role in coordinating a decentralized global WHOIS for the generic top-level domain system." READ MORE

Source: New York Times

Date: 7 Jun 2018

Philippine Police arrest nearly 500 in alleged online fraud

"Philippine police arrested nearly 500 people, including eight Israeli nationals, who they say were involved in an online investment fraud that victimized people overseas, including in Australia and South Africa, police said Thursday. In one of the Philippines' biggest anti-cybercrime busts in years, police chief Oscar Albayalde said 474 Filipino employees and the Israelis were taken into custody following the raid on three buildings in Clark Freeport, a former U.S. Air Force base north of Manila, where the alleged online fraud was committed. The suspects lured victims into investing in foreign stocks in a purportedly flourishing London-based company then took their money through an online app after obtaining their bank account and credit card details, said Chief Superintendent Marni Marcos, who heads the national police Anti-Cybercrime Group." READ MORE

Source: La Tercera

Date: 12 Jun 2018

Ciberataques en Chile: gobierno buscará asesoría internacional y apunta a coordinar a reguladores

"A tres semanas de que el Banco de Chile sufriera un ciberataque en el que bandas internacionales le sustrajeron US$10 millones, el gobierno y los reguladores concretaron ayer dos reuniones para analizar temas relacionados con el inédito robo. […] Definieron dos ejes principales de acción para modernizar y perfeccionar los protocolos de contingencia y el marco regulatorio y de supervisión en ciberseguridad. El primero de ellos consiste en contratar a un organismo internacional para que los asesore "para identificar las brechas en relación con los estándares y recomendaciones internacionales para prevenir y enfrentar los ciberataques que pueden sufren las entidades del mercado financiero, con especial énfasis en los bancos", manifestó Hacienda mediante un comunicado. Como segundo eje, definieron firmar un memorándum de entendimiento (MoU) entre las instituciones integrantes del Grupo de Trabajo (Ministerio de Hacienda, SBIF, CMF, Superintendencia de Pensiones y Banco Central), para compartir información y avanzar algunos objetivos." READ MORE

Source: Reussir Business

Date: 5 Jun 2018

Le Sénégal inaugure le 1er centre de cybersécurité d'Afrique subsaharienne

"Le 1er centre cybersécurité d'Afrique subsaharienne a été inauguré par le Sénégal pour la protection des usagers des services financiers. La cérémonie a été présidée par Aminata Angélique Manga, Ministre de l'Economie solidaire et de la Microfinance, sous la présence des membres de l'APSFD, du Directeur général de Suricate solutions et des autorités du Grand-Duché de Luxembourg à Dakar. Dans un monde marqué par un développement accru du numérique dans les services financiers, la sécurité devient un impératif pour renforcer l'inclusion financière. Pour Mme Aminata Angélique Manga, ce centre vise à faire de la microfinance un secteur clé de l'économie nationale et faire en sorte que l'inclusion financière soit une réalité." READ MORE

Source: Proshare

Date: 7 Jun 2018

Nigeria's Central Bank Mandates All Banks To Comply With Cybercrime Act 2015

"Pursuant to the provisions of Section 44 (S.1and 2) of the Cybercrime [Prohibition, Prevention, etc.], Act 2015, which established the National Cyber Security Fund and mandated the payment of a levy of 0.005% into the Fund Account in the Central Bank of Nigeria, a National Cyber Security Fund account has been opened and domiciled in the Central Bank of Nigeria. Consequently, all banks are hereby directed to comply with the statutory provision for the collection and remittance of the 0.005% levy on all electronic transactions by the businesses specified in the second schedule of the Cybercrime (Prohibition, Prevention, etc.) Act." READ MORE

Source: Agence Ecofin

Date: 11 Jun 2018

Le Niger se lance dans l'élaboration de sa stratégie nationale de cybersécurité

"La République du Niger a décidé de se doter d'un plan d'action approprié pour protéger ses réseaux télécoms et informatiques. Le 7 juin 2018, elle a installé un comité technique chargé de l'élaboration de sa stratégie nationale de cybersécurité, avec prise de fonction immédiate. Du document national de référence en matière de lutte contre la cybercriminalité attendu de cette équipe, dépendra le niveau de préparation futur du pays aux risques inhérents aux technologies de l'information et de la communication en constante évolution. La nécessité de doter le pays d'une feuille de route en matière de cybersécurité s'est imposée au gouvernement nigérien, au regard de l'ampleur que prend la cybercriminalité dans le pays et en Afrique de l'Ouest, avec plusieurs pays voisins présentés comme des nids de brigands numériques." READ MORE

Source: IT Web Africa

Date: 12 Jun 2018

Zambia: civil society, govt clash over cyber security Bills

"Civil society organisations in Zambia […] have demanded that government halt the process of enacting three cyber security Bills. The organisations have accused lawmakers of overlooking their participation in deliberation over the Cyber Security and Cybercrime Bill, Data Protection Bill and Electronic Commerce and Transaction Bill, before these are sent to parliament. They add that the government should rather focus on strengthening existing cyber crime laws instead of introducing 'bills that have been hidden from the public.'" READ MORE

Source: Reuters

Date: 12 Jun 2018

Vietnam lawmakers approve cyber law, tighten rules on Google, Facebook

"Vietnamese lawmakers approved a controversial cybersecurity law on Tuesday, voting amid tight security following weekend protests over other legislation that turned violent in some parts of the communist country. The law, approved by 91 percent of attending lawmakers, would require Facebook, Google and other global technology firms to store locally "important" personal data on users in Vietnam and open offices in the country. The companies have pushed back against the provisions." READ MORE

Latest reports

- Council of Europe, Octopus Conference – Programme, Resources, last updated 15 Jun 2018
- Council of Europe, Snapshot of Council of Europe's approach on Cybercrime and electronic evidence and CyberSouth project, June 2018
- European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, 6 Jun 2018
- ICANN, WHOIS Compliance with GDPR – Reference, last updated 4 Jun 2018
- APWG and Japan Cybercrime Control Center, Revealed Threat of Fake Store, 5 Jun 2018
- UK Government, Investigatory Powers Act 2016 – codes of practice, 12 Jun 2018
- The Spamhaus Project, The 10 Worst Botnet Countries, updated 15 Jun 2018

Upcoming events

- 12-15 June, Belgrade, Serbia – Pilot training session on introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 18-19 June, Tirana, Albania – Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (2nd part), iPROCEEDS
- 18-22 June, Singapore – INTERPOL Instructor Development Course for GLACY+ countries, GLACY+
- 19-21 June, Baku, Azerbaijan - Advisory Mission on international cooperation through 24/7 points of contact and mutual legal assistance, Cybercrime@EAP 2018
- 19-22 June, Cebu, Philippines – Advanced Judicial Training on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers from the ASEAN region, GLACY+
- 26 June, Budapest, Hungary – Coordination mission with CEPOL, CyberSouth
- 27-29 June, London, United Kingdom – 3rd INTERPOL Digital Forensics Experts Group, GLACY+
- 28 June, The Hague, Netherlands – Participation of one delegate from the Philippines in the GFCE Meeting of the WG on Cyber Security Policy and Strategy, GLACY+

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