Cybercrime Digest

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

16-31 March 2018

Source: EU Neighbours

Date: 26 Mar 2018

CyberSouth Launching Conference: a successful start

"The Launching Conference of CyberSouth started on March 21 with a series of sessions on cybercrime policies and strategies in the Southern Neighbourhood Region, and with an overview of the assessment visits conducted last year in the priority countries of the project. The opening of the conference was addressed by Hatem Ferjani, State Secretary, Ministry of Foreign Affairs of Tunisia, and Habib Dababi, State Secretary, Ministry of Communication Technologies and Electronic Economy of Tunisia. […] The Launching Conference of the joint European Union and Council of Europe project, organized in Tunis, Tunisia, allowed countries to exchange views on cybercrime policies and strategies of priority countries under the project, in order to guide project activities, and also to determine the support to be provided through the CyberSouth project." READ MORE

RELATED ARTICLES

Morocco World News, Cybersouth Project Targets Cybercrime in Morocco, 20 Mar 2018
Realités, Tunisie: une conférence internationale pour le lancement du projet CyberSud, 19 Mar 2018

Source: EU Delegation to the Philippines

Date: 20 Mar 2018

Philippines, EU underscores need for international cooperation and dialogue to address cybercrime

"European Union Ambassador Franz Jessen has underscored the need for international cooperation and dialogue to address issues such as cybercrime during the Training of Trainers Course on Cybercrime and Electronic Evidence for Judges, Magistrates and Prosecutors of the ASEAN Region which opened this morning of 20 March 2018 in Manila.[…] Ambassador Jessen expressed his appreciation to the Philippines for its efforts to join the Budapest Convention during the last years, culminating with the passing of the Accession Instrument by the Senate in February this year." READ MORE

Source: The New York Times

Date: 19 Mar 2018

Facebook and Cambridge Analytica explained

"Cambridge Analytica, a political data firm hired by President Trump's 2016 election campaign, gained access to private information on more than 50 million Facebook users. The firm offered tools that could identify the personalities of American voters and influence their behavior. […] The data included details on users' identities, friend networks and "likes." The idea was to map personality traits based on what people had liked on Facebook, and then use that information to target audiences with digital ads. Researchers in 2014 asked users to take a personality survey and download an app, which scraped some private information from their profiles and those of their friends, activity that Facebook permitted at the time and has since banned. […] What Cambridge did was not a data breach, because Facebook routinely allows researchers to have access to user data for academic purposes — and users consent to this access when they create a Facebook account. But Facebook prohibits this kind of data to be sold or transferred 'to any ad network, data broker or other advertising or monetization-related service.'" READ MORE

Source: Lexology

Date: 27 Mar 2018

U.S. Congress Passes CLOUD Act to Facilitate Law Enforcement Access to Overseas Data

“The Situation: The U.S. Congress passed the CLOUD Act amending U.S. surveillance laws to facilitate law enforcement access to the contents of communications and other related data. The Result: U.S. law enforcement authorities can compel production of communications data even if it is stored outside the United States, and certain foreign countries may be eligible to enter into executive agreements with the United States that would permit U.S. service providers to respond to certain foreign orders seeking access to communications data. Looking Ahead: Providers of electronic communications and certain cloud services should be prepared to respond to legal process under the new regime, while both providers and users of their services should consider the implications for their businesses.” READ MORE

Source: MerihNews

Date: 30 Mar 2018

Turkey, The Court of Cassations Pioneering Ruling

“The 16th Penal Chamber of the Court of Cassation reversed the ruling of imprisonment in Samsun because of the use of ByLock app due to the insufficient investigation. The prosecutors demanded up to 15 years imprisonment of Ç.Ç. for allegedly using ByLock and being a member of an armed terrorist organisation. A court sentenced the defendant to 7 years which was also approved by Samsun Provincial Court. The defendant appealed the decision and took the case to the 16th Penal Chamber of the Court of Cassation. The court reversed the ruling. The decision emphasises that the defendant does not confirm using the ByLock app and states that: “…The decision must have been taken after requesting detailed evaluation report for ByLock use, the defendant’s statement and evaluating all these data. It is against the law to issue a ruling based on an insufficient investigation.” READ MORE

RELATED ARTICLES

Reuters, Turkey orders 243 detained on suspected links to Gulen network: Anadolu, 9 Mar 2018

See also: European Court of Human Rights, case of Mehmed Hasan Altan vs Turkey (20 March 2018): “…regarding the contents of the messages exchanged by other individuals via ByLock, the Constitutional Court held that the messages could not in themselves be regarded as significant indications that the applicant had committed an offence…”.

Source: ICANN

Date: 28 Mar 2018

ICANN Requests DPA Guidance on Proposed Interim Model for GDPR Compliance

“In letters to each of the 28 European member states' DPAs and the European Data Protection Supervisor, ICANN asks the authorities to "help ICANN and the domain name registries and registrars to maintain the global WHOIS in its current form, through either clarification of the GDPR, a moratorium on enforcement or other relevant actions, until a revised WHOIS policy that balances these critical public interest perspectives may be developed and implemented." Absent this specific guidance, the integrity of the global WHOIS system and the organization's ability to enforce WHOIS requirements after the GDPR becomes effective will be threatened. ICANN is concerned that continued ambiguity on the application of the GDPR to the global WHOIS may result in many domain name registries and registrars choosing not to publish or collect WHOIS out of fear that they will be subject to significant fines following actions brought against them by the European DPAs.” READ MORE

RELATED ARTICLES

Krebs on Security, Who Is Afraid of More Spams and Scams?, 16 Mar 2018

Source: Reuters

Date: 19 Mar 2018

G20 leaders to hold fire on cryptocurrencies amid discord

"The world's financial leaders gathering in Argentina on Monday are likely to stop short of any specific action aimed at regulating cryptocurrencies such as Bitcoin, amid discord over the approach, sources at the summit told Reuters. Wild swings in the price of Bitcoin, the best known of a myriad of digital currencies issued by private companies, cyber heists involving such assets, and fears they may be used for crime have raised calls for concerted actions by global regulators. Finance ministers and central bankers from the world's 20 largest economies meeting in Buenos Aires will be told on Tuesday that such "crypto assets" do not threaten financial stability but can serve to launder money or finance terrorism and hurt consumers who buy them. However, no action is expected to follow at the summit as policymakers have yet to agree on a common strategy to tackle the issue and some countries, including the United States, are wary of new regulation after a decade of rule-making in the wake of the financial crisis of 2008-2009, the sources said." READ MORE

RELATED ARTICLES The Bangkok Post, Cabinet OKs digital asset draft decrees, 14 May 2018

Source: The Guardian

Date: 20 Mar 2018

Child abuse imagery found within bitcoin's blockchain

"German researchers have discovered unknown persons are using bitcoin's blockchain to store and link to child abuse imagery, potentially putting the cryptocurrency in jeopardy. The blockchain is the open-source, distributed ledger that records every bitcoin transaction, but can also store small bits of non-financial data. This data is typically notes about the trade of bitcoin, recording what it was for or other metadata. But it can also be used to store links and files. Researchers from the RWTH Aachen University, Germany found that around 1,600 files were currently stored in bitcoin's blockchain. Of the files least eight were of sexual content, including one thought to be an image of child abuse and two that contain 274 links to child abuse content, 142 of which link to dark web services." READ MORE

Source: Agencia Fe

Date: 26 Mar 2018

Argentina, es ley la simple tenencia de Pornografía Infantil

"La semana pasada, la Cámara de Diputados convirtió en ley el proyecto que tipifica el delito de tenencia de pornografía infantil, y estipula el agravamiento de las penas para que no sea excarcelable. La iniciativa fue avalada por abrumadora mayoría de los votos: 211 votos a favor y dos abstenciones. […] La normativa, a su vez, establece que las penas se elevarán en un tercio cuando la víctima fuere menor de 13 años. El Dr. Gonzalo Jeanglorges, abogado especialista en Derecho Infromático e Internet, […] contó que "en realidad nosotros desde 2008 teníamos tipificado la pornografía infantil pero en relación a la producción en menores de 18 años, solamente la tenencia estaba tipificada cuando el fin era la distribución o comercialización". "En la Argentina desde noviembre del año pasado incorporó hay un tratado internacional de 2001 que se llama Convenio de Budapest en el cual se exigía que la Argentina adecuara sus normas penales y justamente la tenencia simple de material pornográfico tenía que estar tipificado como delito", agregó Jeanglorges." READ MORE

Source: The Guardian

Date: 18 Mar 2018

Threat of Russian cyber reprisal puts UK finance, power and water on high alert

"Banks, energy and water companies are on maximum alert over the threat of a serious cyber-attack from Moscow as concern continues over the safety of Russian exiles in the UK. Fears that Russia will target Britain's critical national infrastructure have prompted round-the-clock threat assessments by the UK's financial sector, energy firms and GCHQ, the UK's largest intelligence agency, along with the security services MI5 and MI6." READ MORE

Source: Europol

Date: 26 Mar 2018

Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain

"The leader of the crime gang behind the Carbanak and Cobalt malware attacks targeting over a 100 financial institutions worldwide has been arrested in Alicante, Spain, after a complex investigation conducted by the Spanish National Police, with the support of Europol, the US FBI, the Romanian, Moldovan, Belarussian and Taiwanese authorities and private cyber security companies. Since 2013, the cybercrime gang have attempted to attack banks, e-payment systems and financial institutions using pieces of malware they designed, known as Carbanak and Cobalt. The criminal operation has struck banks in more than 40 countries and has resulted in cumulative losses of over EUR 1 billion for the financial industry. The magnitude of the losses is significant: the Cobalt malware alone allowed criminals to steal up to EUR 10 million per heist." READ MORE

Source: Global Voices

Date: 30 Mar 2018

Tunisian MPs Propose Legislation Criminalising 'Cyber Defamation'

"Tunisian members of parliament are proposing a bill that would criminalise online defamation. On 22 March, sixteen legislators from the Nidaa Tounes party in the ruling coalition, along with one independent MP, submitted a proposal to amend the country's penal code by adding two articles on what they call "cyber-defemation'". If adopted, the amendments would prescribe a two-year jail sentence and a fine of three thousand Tunisian dinars against those convicted of publishing content "that could harm public order, good morals, sanctity of the private life, and the honour" of individuals and "official institutions". In their proposal, the MPs argue that the penal code is not "up to date with technological developments, particularly in the information sector" and that there is a need to "protect the Tunisian society" from "behaviours and violations that exceed press freedom" such as insults and abuse." READ MORE

Source: All Africa

Date: 21 Mar 2018

South Africa has the third most cybercrime victims worldwide

"It's certainly true that cybercrime is a worldwide problem, but recent research has shown that South African consumers are bearing the brunt disproportionately, with the country reportedly having the third highest number of cybercrime victims anywhere in the world. It also suffers more attacks than any other African country. South African consumers are losing about R2.2 billion a year to cyber attacks. […] Until very recently, South African had no legislation in place to address cybercrime. However, all that has now changed with the introduction of the Cybercrime and Cyber Security Bill, which has brought South Africa in line with international laws." READ MORE

Source: SMEX

Date: 14 Mar 2018, updated on 22 March 2018

New anti-cybercrime legislation enacted in Syria

"On March 5, the Syrian Council of Ministers passed a new anti-cybercrime bill, creating specialized courts of first instance for cybercrime-related cases. These courts are the lowest level courts (bida'iyya) in the Syrian judicial system and their rulings can be challenged at the Court of Appeal. Shortly after the bill's enactment, the Syrian Ministry of Justice appointed 58 judges to handle these cases. The bill amends Cybercrime Law 17/2012, which penalizes "anyone who incites or promotes crime through computer networks" with prison sentences ranging between one and three years and a fine of up to $1,500, according to the latest Freedom on the Net report on Syria (last updated in May 2017). In the past, those who violated the law were tried by any court within the judicial system or by military tribunals." READ MORE

Source: CNN

Date: 30 Mar 2018

Malaysia's anti-fake news law raises media censorship fears

"With elections around the corner and a years-long financial scandal plaguing Malaysian Prime Minister Najib Razak, many within the country's media, legal fraternity and civil society are worried about the government's intent in introducing the bill. The proposed Anti-Fake News Bill 2018 will give the government sweeping powers to hit those it deems guilty of creating or spreading fake news with jail terms of up to six years and fines that could as high as $130,000. […] At the heart of the problem is a broad definition of what constitutes fake news and who an offender could be." READ MORE

Source: Europol

Date: 29 Mar 2018

20 hackers arrested in EUR 1 million banking phishing scam

"A two-year long cybercrime investigation between the Romanian National Police and the Italian National Police, with the support of Europol, its Joint Cybercrime Action Taskforce (J-CAT) and Eurojust, has led to the arrest of 20 suspects in a series of coordinated raids on 28 March. 9 individuals in Romania and 11 in Italy remain in custody over a banking fraud netted EUR 1 million from hundreds of customers of 2 major banking institutions. The Romanian authorities have conducted 15 house searches, while the Italian National Police ordered the execution of 10 home and computer searches, involving more than 100 Italian policemen." READ MORE

Latest reports

- UNODC, Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, Comments received in accordance with the Chair's proposal for the work plan for the period 2018-2021, March 2018
- US-CERT, Alert (TA18-074A) – Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, 15 Mar 2018
- IETF, The Transport Layer Security (TLS) Protocol Version 1.3, approved on 21 Mar 2018
- BSA, 2018 BSA Global Cloud Computing Scorecard, 6 Mar 2018

Upcoming events

- 3-5 April, Vienna, Austria – UN Intergovernmental Expert Group Meeting on Cybercrime, Cybercrime@Octopus / GLACY+ / iPROCEEDS / Cybercrime@EAP 2018 / CyberSouth
- 4-5 April, Algiers, Algeria – 11th Middle East and North Africa Working Group on Cybercrime for Heads of Units, CyberSouth
- 4-6 April, Colombo, Sri Lanka – Integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, GLACY+
- 6-7 April, Vienna, Austria – T-CY Protocol Drafting Group meeting, Cybercrime@Octopus / iPROCEEDS / Cybercrime@EAP 2018
- 11-12 April, Addis Ababa, Ethiopia – Workshop on cybercrime and electronic evidence for Ambassadors to the African Union Commission of all the African countries, GLACY+
- 11-13 April Kyiv, Ukraine – National workshop to discuss cooperation between CSIRT, law enforcement and private sector from the perspective of cybersecurity strategies, discussion of memorandum of cooperation and online resource, Cybercrime@EAP 2018

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