Cybercrime Digest

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

1-14 February 2018

Source: Council of Europe

Date: 13 Feb 2018

Tunisia invited to join the Budapest Convention on Cybercrime

"Tunisia was invited today to accede to the Budapest Convention on Cybercrime. With Tunisia, 71 States are now either Parties (56), have signed it (4) or been invited to accede (11). Through the project CyberSouth, the Council of Europe and the European Union are supporting Tunisia in further strengthening of legislation and criminal justice capacities to permit the country to become a Party in the near future." READ MORE

Source: Council of Europe

Date: 7 Feb 2018

Malaysian legislation compatible with the Budapest Convention

"Malaysian legislation on cybercrime and e-evidence is sufficiently compatible to request accession to the Budapest Convention, even though further reforms of legislation and capacity building efforts are needed prior to actual accession. This was one of the main conclusions of a "High-level Round Table on the Budapest Convention on Cybercrime", held in Kuala Lumpur, Malaysia, on 6 and 7 February 2018. The meeting was opened by YB Dato' Sri Azalina Othman Said, Minister in the Prime Minister's Department, who invited representatives of 15 public and private sector institutions to engage in consultations on the readiness of Malaysia to join this treaty." READ MORE

Source: Senate of the Philippines

Date: 13 Feb 2018

Philippines, Senate Approves on 2nd Reading the Cybercrime Convention

"The Senate approved today on second reading five treaties, including the Budapest Convention on Cybercrime. Senator Loren Legarda, Chair of the Senate Committee on Foreign Relations, said that the agreements are scheduled for approval on third and final reading on Monday, February 19. Legarda explained that the Budapest Convention on Cybercrime remains the only binding international legal mechanism adopted by countries to address the threats posed by cybercrime. […] The Senator said that the Budapest Convention on Cybercrime will provide the Philippines distinct guideposts on the track towards harmonizing its national laws with prevailing international legal frameworks and practices." READ MORE

Source: BBC

Date: 12 Feb 2018

Criminals hide 'billions' in crypto-cash - Europol

"Three to four billion pounds of criminal money in Europe is being laundered through cryptocurrencies, according to Europol. The agency's director Rob Wainwright told the BBC's Panorama that regulators and industry leaders need to work together to tackle the problem. The warning comes after Bitcoin's value fell by half from record highs in December. […] Mr Wainwright said that Europol, the European Union Agency for Law Enforcement Cooperation, estimates that about 3-4% of the £100bn in illicit proceeds in Europe are laundered through cryptocurrencies." READ MORE

Source: Ministério Pùblico

Date: 7 Feb 2018

Specialists of the Portuguese-speaking Public Prosecution Services discuss cybercrime in Lisbon

"A meeting of the Fórum Cibercrime was held on 7 February, at the Prosecutor General's Office, in Lisbon. The Fórum Cibercrime is the informal meeting of specialists of the Portuguese-speaking Public Prosecution Services dedicated to combating cybercrime, created by the XIV Meeting of Prosecutors General of the Community of Portuguese-speaking Countries (CPLP) […]: Angola, Brazil, Cape Verde, Guinea Bissau, Mozambique, São Tome and Principe, Timor-Leste and Macao – the latter as an observer. […] The general objective of this Fórum is to share information on the legal framework of the various Portuguese-speaking countries in cybercrime. The meeting was supported by the European Union and the Council of Europe, through the GLACY+ Project." READ MORE

RELATED ARTICLES
Ministério Público Portugal, Meeting of CiberRede/CiberRed, 5 Feb 2018
Ministério Público Portugal, International Conference on Cybercrime, 6 Feb 2018

Source: Europol

Date: 5 Feb 2018

International crackdown on anti-spyware malware

"A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. This case was investigated by the South West Regional Organised Crime Unit and coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America. Once installed upon a victim's computer, a user of the Luminosity Link RAT was free to access and view documents, photographs and other files, record all the keystrokes entered and even activate the webcam on the victim's computer – all of which could be done without the victim's knowledge." READ MORE

Source: Reuters

Date: 7 Feb 2018

U.S. shuts down transnational cyber crime ring responsible for more than $530 Million losses

"The U.S. Justice Department announced one of its largest-ever takedowns of a global cyber crime ring on Wednesday, saying it had indicted 36 people accused of trafficking in stolen identities and causing more than $530 million in losses to consumers. The cyber crime network, operating as an online discussion forum known as "Infraud," ran a sophisticated scheme that facilitated the purchase and sale of Social Security numbers, birthdays and passwords that had been stolen from around the world. The group worked under the slogan "In Fraud We Trust" and was created in 2010 by Svyatoslav Bondarenko, a 34-year-old Ukrainian. In launching it, the indictment alleges he referred to online forum as a "comfortable and safe" place to "bring together professional people for who carding and hacking become a lifestyle." READ MORE

RELATED ARTICLES
U.S. Department of Justice, Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes, 7 Feb 2018

Source: The Register

Date: 9 Feb 2018

As GDPR draws close, ICANN suggests 12 conflicting ways to cure domain privacy pains

"Incoming European privacy laws which carry a global impact for anyone doing business in the Union are continuing to cause an epic policy meltdown at internet overseer ICANN. This week the European Commission responded to the US-based organization's latest efforts to resolve a stark conflict between the domain name system's Whois service and the General Data Protection Regulation (GDPR), that will come into force this May. "Given the level of abstraction of the models, it is difficult to assess the scope and impacts of the proposed approaches," wrote the EC's director-general of technology and communications. "The Commission therefore encourages ICANN to further develop possible options in cooperation with the community in order to balance the various legal requirements, needs and interests."." READ MORE

RELATED ARTICLES
Euractiv, Bruxelles veut restreindre l'accès aux registres publics des sites Internet, 9 Feb 2018

Source: The Hill

Date: 6 Feb 2018

U.S. Senate to discuss bipartisan bill to clarify cross-border data policies

"Sen. Orrin Hatch on Monday introduced a bill aimed at creating a clearer framework for law enforcement to access data stored in cloud computing systems. Hatch's bill is aimed at making it easier for U.S. officials to create bilateral data sharing agreements that allow them to access data stored overseas and also for foreign law enforcement to access data stored on U.S. firms' servers. […] Federal law currently doesn't specify whether the government can demand that U.S. companies give it data they have stored abroad. The CLOUD Act would amend this, likely impacting Microsoft's pending Supreme Court case over data it has stored in Ireland. A lower court has previously ruled that Microsoft doesn't have to turn over data stored overseas, following a request for it to do so by the Department of Justice." READ MORE

RELATED ARTICLES
Bloomberg, Tech Giants Back U.S. Bill on Cross-Border Data Searches, 7 Feb 2018

Source: Reuters

Date: 13 Feb 2018

Russia says hackers stole more than $17 million from its banks in 2017

"Hackers stole more than 1 billion roubles ($17 million) from Russian banks using the Cobalt Strike security-testing tool in 2017, a central bank official said on Tuesday. Russia is under intense scrutiny over cyber crime following allegations hackers backed by Moscow have attacked targets in the United States and Europe, accusations the Kremlin has repeatedly denied. Russian authorities are now keen to show that Russia too is a frequent victim of cyber crime and that they are working hard to combat it. Central bank Deputy Governor Dmitry Skobelkin told an information security conference in the Russian city of Magnitogorsk that 21 "waves of attacks" using Cobalt Strike had been recorded in 2017. "More than 240 credit organizations were hit by the attacks, 11 of which were successful. The amount stolen was more than 1 billion roubles," he said." READ MORE

Source: Pattaya Mail

Date: 2 Feb 2018

Thai army ramping up cyber security

"Deputy Prime Minister and Defense Minister Gen Prawit Wongsuwan chaired a defense council meeting this week to follow up on the military's cyber security measures. The meeting was also attended by army chiefs and other high-ranking military officers. They discussed topics related to developing an effective cyber-security strategy, enhancing the army's capacity to deal with cyber threats, and establishing a cyber defense command center. The Ministry of Defense is also planning to recruit 1,000 cyber security experts to guard against all types of online threats." READ MORE

Source: IT Web Africa

Date: 9 Feb 2018

Zambia tables legislation to regulate social media

"Zambia's Transport and Communications Minister Brian Mushimba has confirmed the country's parliament will review three bills designed to regulate internet usage and social media: the cybersecurity and cybercrime bill, e-commerce bill and data protection bill. In April last year President Edgar Lungu openly challenged Zambia's Information and Communication Technology Regulatory Authority (ZICTA) to control what he believed to be the threat of social media abuse. In January, presidential spokesperson Amos Chanda communicated with the Inspector General of the Zambia police, Kakoma Kanganja and requested intervention to curtail what he described as 'repeated forgery and altering of state house statements on social media.'" READ MORE

Source: New Era

Date: 7 Feb 2018

Namibia a safe haven for cybercriminals

"An exploratory research study on knowledge, attitudes and practices of ICT use and online protection risks by adolescents in Namibia showed that 68 percent of children reported having seen sexual content they did not wish to see, while 31 percent had been sent sexually explicit images of people they didn't know, and 29 percent had seen child sexual abuse material online. The study revealed that up to 80 percent of all cybercrimes go unreported due to the lack of awareness about cybercrimes. While these findings reveal that violence and exploitation of children in Namibia frequently have an online component and contribute to creating an unsafe environment for children, only a very minimum number of cases have been successfully prosecuted as no legislation is in place that comprehensively criminalises child pornography and other cybercrimes." READ MORE

Source: Daily Nation

Date: 13 Feb 2018

Kenya proceeds with caution on the cybercrimes bill

"The Computer and Cybercrimes Bill of 2017 is before Parliament and undergoing public consultations. Whereas it does contain contentious clauses, we must be careful not to throw out the baby with the bathwater. This is because the Cybercrimes Bill is one of the four pending bills that are required to usher in a true digital economy for Kenya. The other three are the Data Protection Act, the Electronic Transactions Act and the Copyright Act. A quick glance at the proposed Computer and Cybercrime Bill shows that it is based on the European Union benchmark, commonly known as the Budapest Convention on Cybercrime. […] In general, the Kenyan cybercrime bill has tried to be consistent with the Budapest Convention. […] On a broad level, the bill lacks the supporting governance framework under which it can be adopted. Specifically, issues to do with capacity building in the police and judicial wing are not covered, meaning that implementation of the law will face serious challenges." READ MORE

Source: La Prensa

Date: 10 Feb 2018

Honduras, adherirse a Convenio de Budapest sobre ciberdelincuencia sugieren congresistas

"En el dictamen de la Ley Nacional de Ciberseguridad y Medidas de Protección ante los Actos de Odio y Discriminación en Internet y Redes Sociales, la comisión especial multipartidaria del Congreso Nacional recomendó el viernes que el país se adhiera al Convenio de Budapest sobre ciberdelincuencia. En la exposición de motivos, la comisión multipartidaria recomienda que se inicien las acciones por parte del Poder Ejecutivo para la adhesión de Honduras al Convenio sobre la Ciberdelincuencia, de Budapest, suscrito el 23 de noviembre del 2001. […] A partir del 28 de octubre de 2010, treinta Estados firmaron, ratificaron y se adhirieron a la convención, mientras que otros 16 rubricaron la convención, pero no la ratificaron." READ MORE

Source: Reuters

Date: 5 Feb 2018

India to bar cryptocurrencies from its payments system: finance ministry official

"India is planning steps to ensure cryptocurrencies are illegal within its payments system, while at the same time appointing a regulator to oversee unregulated exchanges that trade in "crypto assets," a finance ministry official said on Monday. A panel set by the government to look into issues relating to cryptocurrencies is expected to submit its report in the current fiscal year, ending on March 31, S.C. Garg, Economic Affairs Secretary, told CNBC TV18 news channel. "The government will take steps to make it illegal as a payment system," he said at a post-budget event telecast by the news channel, adding the trading of "crypto assets" at the unregulated exchanges would be regulated." READ MORE

RELATED ARTICLES
Valuewalk, Pakistan Government To Declare Cryptocurrency Illegal, 10 Feb 2018

Source: The Phnom Penh Post

Date: 5 Feb 2018

Telecoms regulator to investigate internet providers for snubbing Cambodia Daily ban

"Cambodia's Telecommunications Regulator (TRC) said today that it will investigate internet service providers (ISP) that have not blocked the Cambodia Daily website, warning that those who fail to comply with a now months-old order could lose their licences. Government documents, which came to light yesterday, show the Ministry of Posts and Telecommunications, at the request of the General Department of Taxation, ordered ISPs to block access to the Cambodia Daily IP address, as well as its Facebook page and Twitter account. Only a handful of ISPs seem to have complied with the government request. MekongNet and Sinet KH confirmed the block, and access also appeared to be restricted through the provider Online. The Daily was forced to close in September last year after it was handed a $6.3 million tax bill, which many observers contend was used to silence an outlet often critical of the government." READ MORE

Latest reports

- Council of Europe, Summary report of the 2nd Meeting of the T-CY Protocol Drafting Group, 2 Feb 2018
- ENISA, Information Sharing and Analysis Center (ISACs) - Cooperative models, 14 Feb 2018
- ENISA, Public Private Partnerships (PPP) - Cooperative models, 14 Feb 2018
- ENISA, European Cyber Security Month 2017 – Deployment Report, 6 Feb 2018
- ICANN, Data Protection/Privacy Update: Latest Developments, 14 Feb 2018
- UK National Cyber Security Center, Active Cyber Defence - One Year On, 6 Feb 2018

Upcoming events

- 15-16 February, Skopje, "the former Yugoslav Republic of Macedonia", Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (1st part), iPROCEEDS
- 16 February, Beirut, Lebanon – Basic judicial training course on cybercrime and electronic evidence, CyberSouth
- 19-21 February, Colombo, Sri Lanka – Advisory mission on the set-up of the Cybercrime Division at the CID, GLACY+
- 19-22 February, Rome, Italy – Participation of two Ghanaian officers in the Drug Online Course, organized by the Central Directorate for Antidrug Services (C.D.A.S.) and the Multiagency College of Advanced Studies for Law Enforcement Officials, Cybercrime@Octopus
- 20 February, Brussels, Belgium – CT MENA coordination meeting, organized by DG DEVCO and DG NEAR, CyberSouth
- 20-22 February, Tbilisi, Georgia – National workshop to discuss cooperation between CSIRT, law enforcement and private sector from the perspective of cybersecurity strategies/Workshop to expand, complete and maintain the online tool on public/private cooperation, Cybercrime@EAP 2018
- 26-27 February, Chisinau, Moldova – Workshop on legal and practical aspects of LEA/ISP cooperation, Cybercrime@EAP 2018
- 26-28 February, Kathmandu, Nepal – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, GLACY+
- 27 February-2 March, Kenitra, Morocco – Introductory ToT on cybercrime and electronic evidence for Judiciary Police, GLACY+
- 28 February-2 March, Chisinau, Moldova, National workshop to discuss cooperation between CSIRT, law enforcement and private sector from the perspective of cybersecurity strategies/Parallel workshop on legal and technical aspects of LEA/ISP cooperation/Workshop to expand, complete and maintain the online tool on public/private cooperation, Cybercrime@EAP 2018
- 28 February, Brussels, Belgium – Second Conference of the EuroMed Justice IV, CyberSouth