Cybercrime Digest

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

1-15 October 2018

Source: African Union

Date: 16 Oct 2018

The First African Forum on Cybercrime opens today in Addis Ababa

"The African Union Commission, together with a number of partnering organisations, holds the first continent-wide African Forum on Cybercrime from 16 to 18 October 2018 in Addis Ababa, Ethiopia bringing together more than 250 delegates from across the continent. […] The African continent shows one of the fastest growth rates in Internet users worldwide, with digital connectivity that has almost tripled in the past five years. Cyberspace has become an essential tool for communication, innovation, social development and economic progress across the board. On the other hand, both government institutions and companies in Africa have been facing an increasing number of cyber-attacks, in line with global trends. "[…] It is our task and collective responsibility to build a Safe, Secure, Trustworthy and Inclusive Cyberspace for the benefit of all African people and States" said the Commissioner for Infrastructure and Energy, H.E. Dr. Amani Abou-Zeid, speaking ahead of the Forum. On his part, the Deputy Head of the European Union Delegation to the African Union, Mrs. Anna Burylo, said "[…] The evolution of information communication technology has seen in parallel the development of criminal activity that threatens citizens, businesses, governments and critical infrastructures alike: cybercrime. It is a borderless problem… and it needs to be tackled jointly. The European Union therefore strongly believes that we need to work together at all levels to address it and we invest in international cyber cooperation in parallel with our internal efforts for cybersecurity". "[…] The need for international organisations to join forces and enable governments and societies to meet the challenge of cybercrime has been recognised for many years. This Forum is a crucial step in this direction", further emphasized Alexander Seger who is the Executive Secretary of the Committee of the Budapest Convention on Cybercrime at the Council of Europe." READ MORE

RELATED ARTICLES

African Union/ Council of Europe/ INTERPOL/ UNODC/ US/ UK/ Commonwealth Secretariat, Joint press release, 16 Oct 2018

Agency Report, Internet connectivity triples in Africa amid rising cybercrime, 16 Oct 2018

Source: Council of Europe

Date: 9 Oct 2018

Workshop on the Budapest Convention in Jordan

"On 8-9 October 2018, in the framework of CyberSouth project, a workshop on legislation on cybercrime and electronic evidence took place in Amman, Jordan. The activity was organised by the Jordan Armed Forces and the participants were from the Ministry of Foreign Affairs, Ministry of Justice, Judicial Council, Judicial Institute, Public Security Department, Ministry of Telecommunication, and the Central Bank of Jordan. The workshop was aiming to bring together the relevant authorities involved in legislative process and law enforcement with responsibilities in enforcing the cybercrime legislation, to discuss about Budapest Convention as international legislative standard on this area and national legislation from Jordan." READ MORE

Source: European Commission

A Europe that Protects: Commission calls for decisive action on security priorities

Date: 10 Oct 2018

"Today, the European Commission is reporting on the progress made towards an effective and genuine Security Union, calling on the European Parliament and the Council to finalise their work on priority security initiatives as a matter of urgency. […] While a number of legislative proposals made by the Commission have now been approved, there are still many important files that need to be finalised as a matter of urgency before the European Parliament elections in May 2019. The Commission therefore calls for acceleration of this work and a swift adoption of the outstanding files, in particular: […] Fighting cross-border crime: to help police and judicial authorities to track down leads online and across borders, the Commission proposals on electronic evidence should be agreed before the May 2019 elections. The Commission also invites the European Council together with the European Parliament to extend the competence of the European Public Prosecutor's Office (EPPO) to include the investigation of cross-border terrorist offences." READ MORE

Source: African Daily Voice

Le Niger autorise l'adhésion à la Convention sur la cybercriminalité

Date: 13 Oct 2018

"Le parlement nigérien a autorisé vendredi, le projet d'adhésion du pays à la convention sur la cybercriminalité signée le 20 janvier 2003 à Strasbourg par les Etats membres du Conseil de l'Europe et les autres Etats membres signataires. Selon le gouvernement, en adoptant le projet de texte le 2 août dernier, cette convention est un instrument juridique qui vise la réalisation de plusieurs objectifs, notamment 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, la coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, font également partie des objectifs visés par cette convention." READ MORE

Source: The Guardian

Facebook faces $1.6bn fine and formal investigation over massive data breach

Date: 3 Oct 2018

"The Irish Data Protection Commission has opened a formal investigation into a data breach that affected nearly 50m Facebook accounts, which could result in a fine of up to $1.63bn. The breach, which was discovered by Facebook engineers on Tuesday 24 September, gave hackers the ability to take over users' accounts. It was patched on Thursday, the company said. "The investigation will examine Facebook's compliance with its obligation under the General Data Protection Regulation (GDPR) to implement appropriate technical and organisational measures to ensure the security and safeguarding of the personal data it processes," the commission said in a statement on Wednesday. The commission regulates Facebook's adherence to GDPR, a European law that strengthens the privacy protections of individuals and introduces harsh penalties for companies that fail to protect user data. […] Shortly after the Irish Data Protection Commission announced its investigation, the Spanish Data Protection Agency announced it would collaborate on the investigation." READ MORE

Source: The Guardian

Date: 3 Oct 2018

Russia accused of cyber-attack on chemical weapons watchdog

"A Russian cyber-attack on the headquarters of the international chemical weapons watchdog was disrupted by Dutch military intelligence just weeks after the Salisbury novichok attack, it emerged on Thursday, amid fresh revelations of spying that escalated the diplomatic war between the west and Vladimir Putin. The incident, which was thwarted with the help of British intelligence officials, came after the Sandworm cybercrime unit of the Russian military intelligence agency GRU had attempted unsuccessfully to hack the UK Foreign Office in March and the Porton Down chemical weapons facility in April. Jeremy Hunt, the foreign secretary, said on Thursday that Moscow could face further sanctions as a result of an astonishingly detailed evidence trail laid out in the Netherlands, the UK and the US." READ MORE

Source: The Brussels Times

Date: 21 Sep 2018

New evidence that hacking of Proximus was work of British intelligence

"According to a report in De Tijd, the investigation has turned up new evidence to back up what was immediately suspected at the time – that the British government's listening station GCHQ (photo) had hacked into Proximus systems to listen in on communications with Belgacom (as the company was then known) and a subsidiary BICS, which provided communication services via roaming. The discovery of the hacking ended up costing Belgacom €50 million in improving security. One of the methods used was to break into the computers of security personnel using fake LinkedIn messages. Both the federal prosecutor and justice minister Koen Geens have refused to confirm or deny the Tijd report. Geens would go no further than to promise to lay the report before the National Security Council once it was delivered to him." READ MORE

Source: Deepdotweb

Date: 15 Oct 2018

Australian Anti-Encryption Bill Moving Forward Despite Objections from Tech Experts

"On September 10th the deadline passed for public comments on a draft version of Australia's proposed Assistance and Access bill. This is a piece of anti-encryption legislation that is currently being considered by legislators in the Australian House of Representatives. The Department of Home Affairs received over 15,000 comments on the draft of the anti-encryption bill. Many non-profit organizations, businesses, government agencies, and individuals submitted comments on the draft of the Assistance and Access bill, including Access Now, the Internet Architecture Board, Digital Rights Watch, the Asia Cloud Computing Association, and Human Rights Watch among other organizations and individuals. […] The Assistance and Access bill would allow Australian law enforcement to demand that a company, organization, or individual provide them with technical assistance in accessing encrypted communications. For example, if the bill were to be enacted, law enforcement could request that a website install spyware, or they could force a software developer to put a backdoor into his apps. The bill would create new government orders, known as a Technical Assistance Request, Technical Assistance Notice, and Technical Capability Notice, all of which would come with a penalty of five years in prison for anyone who discloses that they have received one of these requests or notices." READ MORE

Source: The New York Times

Date: 15 Oct 2018

A Genocide Incited on Facebook, With Posts From Myanmar's Military

"They posed as fans of pop stars and national heroes as they flooded Facebook with their hatred. One said Islam was a global threat to Buddhism. Another shared a false story about the rape of a Buddhist woman by a Muslim man. The Facebook posts were not from everyday internet users. Instead, they were from Myanmar military personnel who turned the social network into a tool for ethnic cleansing, according to former military officials, researchers and civilian officials in the country. […] While Facebook took down the official accounts of senior Myanmar military leaders in August, the breadth and details of the propaganda campaign — which was hidden behind fake names and sham accounts — went undetected. The campaign, described by five people who asked for anonymity because they feared for their safety, included hundreds of military personnel who created troll accounts and news and celebrity pages on Facebook and then flooded them with incendiary comments and posts timed for peak viewership." READ MORE

Source: The Voice Africa

Date: 12 Oct 2018

Ghana Loses Over $90m to Cybercrime

"Head of the Cybercrime Unit, Ghana Police Criminal Investigation Department, Dr Herbert Gustav Yankson has disclosed that, Ghana has lost over $90million to cybercrime. This is staggering when compared to the loss of $67 million in 2017. According to him, cyber crime is affecting Ghana's economy and as such efforts must be put in place to fight the menace. Some of the crimes include MoMo fraud, phishing and intrusion. The suspects mainly used unauthorized SIM card swap, stolen pin codes and malware to exploit the system. Dr Yankson spoke at length about the SIM card swap and the various tricks such as "the sick child story, police arrest, call credit, spirituality, identity theft, online false investments, job scams, among others" used to commit crimes. […] Dr Yankson said the National Identification System should have access to the telecoms, a special court should be allotted to deal with cybercrime, and called for the prosecution of agents selling already registered SIMs and others to combat cybercrime." READ MORE

Source: The Southern Times

Date: 1 Oct 2018

Cybercrime: elephant in the Namibian House

"Namibia has been advised to speed up the passing of the overdue Cybersecurity Act to pave way for law enforcement agencies and law lords to be able to investigate and prosecute cybercrimes being committed in the country. Namibia has been known as a safe haven for cybercriminals. Many cybercriminals who committed cybercrimes are still roaming freely in the country as there is no legal framework to prosecute them. Speaking during a Cyber Security Workshop for parliamentarians […], Pravesh Behari, a Cybercrime Investigator for Mauritius Police Cybercrime Unit, […] advised Namibia to fast-track the passing of Cybercrimes Bill to give law enforcement guides on how to identify threats, defend against vulnerabilities, investigate incidents […]. He said the absence of cybercrime laws put pressure on law enforcement agencies tasked with investigating various forms of such crimes and cyber threats coming from criminals and state actors alike. […] Once the cybercrime law became effective, it would give guidance to law enforcement officials to be proficient in collecting, handling, and securing this type of evidence and its many novel forms." READ MORE

Source: Namibian

Date: 1 Oct 2018

SADC, laws on cybercrime in the Southern African Region inadequate

"The Southern African Development Community's deputy secretary for regional integration expressed concern at the increase of cybercrime due to enhanced information technology and communication. Thembinkosi Mhlongo, who was addressing the joint SADC session of ministers of information technology and communication, transport and meteorology last Thursday, said the laws are inadequate to combat this rising phenomenon. [...] "At the moment, cybercrime in Africa is growing faster than on any other continent. I understand that all SADC member states either have transposed the SADC harmonised cybersecurity model laws, or have cybersecurity legal frameworks in the workplace. Having the best in place is not enough, support should be given to institutions and networks that fight cybercrime, she said." READ MORE

Source: The News Guru

Date: 1 Oct 2018

Nigeria Communications Commission, Judiciary, to jointly fight cybercrime

"The Nigerian Communications Commission (NCC) on Wednesday called for the cooperation and contributions of the judiciary to checkmate rising cases of cybercrime in the country. The Executive Vice Chairman of NCC, Prof. Umar Danbatta, made the plea in Lagos during the "2018 Annual Workshop for Judges on Legal Issues in Telecommunication''. He said that in spite of the country's positive achievements in digitalisation, the country was still facing issues concerning cyber security, information and data protection. "Cyber criminals have continued to develop new strategies to circumvent cyber security, regardless of measures put in place to checkmate their acts. "It is necessary to discuss the admissibility of electronic evidence toward the successful prosecution of such cyber criminals. "As such, the commission recognises the need for the judicial system to be part of those making contributions to checkmate the issue of cybercrime." READ MORE

Source: South China Morning Post

Date: 5 Oct 2018

Chinese police get power to inspect Internet Service Providers

"China has issued a new regulation setting out wide-ranging police powers to inspect internet service providers and users, as the government tightens its grip on the country's heavily restricted cyberspace. Under the new rule, effective from November 1, central and local public security authorities can enter the premises of all companies and entities that provide internet services and look up and copy information considered relevant to cybersecurity. The regulation was issued by the Ministry of Public Security last month and released on its website on Sunday. It comes more than a year after a controversial cybersecurity law was introduced that has caused widespread concern among foreign companies operating in China." READ MORE

Latest reports

- Council of the European Union, Outcome of the 3641st Council meeting - Justice and Home Affairs, 11-12 Oct 2018
- European Cyber Security Month/ Europol, Take control of your digital life. Don't be a victim of cyber scams!, October 2018

- European Cyber Security Month/ ENISA, Get Cyber Skilled! Support for parents, teachers, guardians, role models and community leaders to develop cybersecurity education and skills in young people, October 2018
- ENISA, Annual Report Trust Services Security Incidents 2017, 8 Oct 2018
- Australian Government and Australian Cyber Security Center, Joint report on publicly available hacking tools, October 2018
- El Djeich, Cyber-sécurité – Une priorité pour l'Union africaine, pp. 42-47, October 2018
- FireEye, APT38, Un-usual suspects, October 2018

Upcoming events

- 22-26 October, Baku, Azerbaijan – Joint training of 24/7 points of contact and other SPCs from investigative agencies with the use of ECTEG materials (Azerbaijan, Georgia, Ukraine), Cybercrime@EAP2018
- 23 October, Accra, Ghana – Training for Justices of Supreme Court and participation in the Criminal Justice Sector Forum on Cybercrime, Cybercrime@Octopus
- 25 October, Accra, Ghana – Special training on cybercrime/cybersecurity for selected members of the Parliament, GLACY+
- 25-26 October, Santo Domingo, Dominican Republic – Participation in the International Congress on Cybercrime organized by the Judicial School of Dominican Republic, GLACY+
- 29 October – 2 November, Chisinau, Moldova – National Cybercrime Cooperation Forum with participation of law enforcement and Internet industry (contribution to Cyber Week MD), Cybercrime@EAP2018
- 29 October – 2 November, Colombo, Sri Lanka – ECTEG Course, Cybercrime and digital forensics specialized training for law enforcement officers, 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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime