Cybercrime Digest

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

1-15 April 2018

Source: African Union

Date: 12 Apr 2018

African Union Commission and Council of Europe Join Forces on Cybersecurity

"The African Union Commission and the Council of Europe jointly organized a workshop on cyber security and cybercrime policies today at the African Union Headquarters for African Diplomats based in Addis Ababa, Ethiopia as part of the ongoing collaboration between the two institutions. The overall objective of the workshop was to bring together the diplomatic community of the African countries to discuss Cybersecurity matters and further raise awareness on the importance of political, legislative and diplomatic efforts, cooperation and commitment necessary in tackling the inherent cross-border nature of cyber-attacks and cyber crime. […] Organized by the African Union Commission and the Council of Europe's Cybercrime Programme Office, the meeting brought together 50 participants including representatives of the Permanent Representative Committees from AU Member States. The European Union is supporting the initiative through the project "Joint EU-CoE Global Action on Cybercrime extended" (GLACY+). The organizers closed the workshop by pronouncing their commitments to accelerate their partnership on cyber security, namely on the organization of the first African Forum on Cybercrime, which will be held in Addis Ababa on 16-18 October 2018. The Forum's main objective will be to promote a coherent approach on cybercrime and related criminal justice issues in Africa." READ MORE

Source: Europol

Date: 9 Apr 2018

Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 Million from drug trafficking

"Operation Tulipan Blanca, coordinated by Europol and conducted by the Spanish Guardia Civil with the support of the Finnish authorities and Homeland Security Investigation of US, has seen 11 arrests and 137 individuals investigated. Members of a crime ring laundered money earned by other organised crime groups, who made their money selling drugs, by using credit cards and cryptocurrencies. The criminals based in Spain were contacted by drug traffickers to launder money obtained from their illegal activities. They picked up the illicit proceeds in cash, which were then split into small quantities to be deposited into hundreds of third bank accounts." READ MORE

Source: Reuters

Date: 3 Apr 2018

Microsoft calls for dismissal of U.S. Supreme Court privacy fight

"Microsoft Corp on Tuesday backed the Justice Department's request that the U.S. Supreme Court dismiss a case pitting the two against each other over whether prosecutors can force technology companies to hand over data stored overseas after Congress passed a law that resolved the dispute. The justices heard arguments in the high-profile case on Feb. 27, but President Donald Trump on March 22 signed legislation that makes clear that U.S. judges can issue warrants for such data while giving companies a way to object if the request conflicts with foreign law." READ MORE

Source: Ministerio de Justicia y del Derecho, Gobierno de Colombia

Date: 4 Apr 2018

Colombia, a tercer debate proyecto de ley que busca la aprobación del convenio sobre la ciberdelincuencia

"La Plenaria del Senado de la República aprobó con 64 votos a favor y en segundo debate, el Proyecto de Ley 58 de 2017 por medio del cual se aprueba el convenio sobre la ciberdelincuencia adoptado el 23 de noviembre de 2001 en Budapest. Esta iniciativa radicada el 1 de agosto de 2017 por el Ministerio de Justicia y del Derecho, el Ministerio de Relaciones Exteriores, el Ministerio de Defensa Nacional y el Ministerio de las Tecnologías de la Información y las Comunicaciones, busca ponerle fin a los múltiples ataques y peligros evidenciados en el ciberespacio. El Convenio de Budapest es el primer tratado internacional que aborda la definición de los delitos cometidos a través de redes informáticas, incluyendo la pornografía infantil y la violación a los derechos de autor. En el caso del Estado colombiano, desde el año 2011 ha realizado acciones para enfrentar de forma efectiva la ciberdelincuencia." READ MORE

Source: Open Gov Asia

Date: 12 Apr 2018

New Zealand announces comprehensive refresh of cybersecurity approach

"New Zealand's Broadcasting, Communications and Digital Media Minister Clare Curran has announced a comprehensive refresh of the country's approach to cyber security. This is being done in view of the increasing number and sophistication of cyber threats and the opportunities for criminals and other states to gain advantage and cause harm in New Zealand. New Zealander's widespread use of connected devices and the security challenges of emerging technology are intensifying the problems. The National Cyber Security Centre estimates that advanced cyber threats could potentially cause $640m harm annually to New Zealand's organisations of national significance. […] Work is now underway - led by the National Cyber Policy Office and Ministry of Justice - to outline what measures might be required to bring New Zealand's laws and investigative processes in line with the Council of Europe Convention on Cybercrime (Budapest Convention). The Cabinet will consider whether New Zealand should formally express interest in accession to the Convention, and the steps towards accession." READ MORE

Source: Le Soleil

Date: 11 Apr 2018

Gestion des données numériques : Comment le Sénégal gère les données numériques de ses citoyens

"Le développement des technologies de l'information et de la communication (TIC) a ouvert à l'économie sénégalaise et à notre vie sociale deux champs différents. L'un est le versant positif avec des opportunités prometteuses en termes d'efficience, de compétitivité et d'inclusivité. Le second versant en appelle à des questionnements. […] Dès 2008, le Sénégal a adopté un ensemble de lois portant sur le cyberespace, ainsi que leurs décrets d'application (la loi n° 2008-08 relative aux transactions électroniques ; la loi n° 2008-10 relative à la loi d'orientation sur la société de l'information (LOSI) ; la loi n° 2008-11 relative sur la cybercriminalité ; la loi n° 2008-12 relative à la protection des données personnelles ; la loi n° 2008-41 relative à la Cryptologie). […] Dans ce cadre, le Sénégal a adhéré à la convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et aussi ratifié à la Convention de Budapest sur la cybercriminalité." READ MORE

Source: El Moudjahid

Date: 7 Apr 2018

Lutte contre la cybercriminalité dans la région Mena: appel à la mise en place de stratégies communes

"Le directeur général de la Sûreté nationale, le général-major, Abdelghani Hamel, a appelé, jeudi à Alger, à l'impératif de poursuivre les efforts entre les pays du Moyen-Orient et de l'Afrique du Nord (Mena) à travers la mise en place de stratégies «communes et efficaces» pour faire face aux défis de la cybercriminalité menaçant les citoyens et les institutions. «Compte tenu du danger émanant de la cybercriminalité, toutes les parties concernées doivent œuvrer constamment à la mise en place de stratégies efficaces et périodiquement actualisées en vue de faire face à cette criminalité, notamment que l'espace cybernétique exige des efforts permanents pour construire la confiance numérique nécessaire», a indiqué Hamel, dans une allocution à l'occasion de la clôture des travaux de la 11e réunion des chefs d'unités de lutte contre la cybercriminalité venus des pays du Moyen-Orient et d'Afrique du Nord, lue en son nom par le directeur de la police judiciaire, Ali Ferrgh." READ MORE

Source: New Era

Date: 11 Apr 2018

SADC strengthens cybercrime policies

"Law enforcement officers from Namibia, Botswana, Malawi, Mozambique, Seychelles, Swaziland and Zambia yesterday gathered in Windhoek to share ideas and strengthen Southern Africa's cyber securities policies. The three-day workshop, organised by the United States Department of Justice, is to focus on techniques for using cyber tools and methods to investigate crime, as well as how to collect and analyse digital evidence. Additionally, participants will explore some of the legal and procedural issues related to using electronic evidence in criminal proceeding. […] Effective tools and techniques for capturing electronic evidence are vital to law enforcement in the 21st Century. Cyber investigation cannot be effective without international cooperation. Investigating cybercrime and collecting electronic evidence are, by their very natures, transnational activities." READ MORE

Source: Daily Nation

Date: 15 Apr 2018

Kenya needs comprehensive cybercrimes law

"Kenya is currently in the process of enacting a Computer and Cybercrimes law to curb illegal activity conducted through a computer system. These crimes include hacking, credit card theft, cyber terrorism, electronic bullying and stalking, identity theft and creating and distributing child pornography. It coincides with Kenya's leading standing in ICTs that has transformed internet connectivity to one of the best in the world […]. Internationally, it has been understood that cybercrime laws need to provide legal sanctions against breach of confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud – and content-related offences such as the criminalisation of child pornography. Countries are also required to setup procedural requirements for investigation and prosecution of cybercrimes, including orders for preservation, production, search and seizure of computer data. Such guidelines are important to ensure that states do not delve into legal sanctions that unjustifiably infringe on fundamental rights such as freedom of expression, right to information and privacy, or sanctions that are already well catered for in several penal provisions." READ MORE

RELATED ARTICLES

Citizen Ke, Cyber attacks cost Kenya Sh20bn in 2017, 11 Apr 2018

Source: Journal de Brazza

Date: 2 Apr 2018

12 800 attaques de cybercriminalité subies par le Cameroun

"Le Cameroun a subi 12 800 attaques liées à la cybercriminalité en 2017, d'après des statistiques publiées lundi par l'Agence nationale des technologies de l'information et de la communication (ANTIC).Menée dans divers secteurs, cette cybercriminalité a eu des conséquences énormes sur l'économie nationale. Dans la foulée, l'ANTIC liste des stratégies développées par des hackers, entre autres, le « scamming » c'est-à-dire, l'escroquerie financière sur Internet, le « skimming » qui porte sur la fraude à la carte bancaire, la fraude à la Simbox c'es-à-dire répondant au boîtier électronique utilisé pour se faire facturer le trafic téléphonique international aux prix du tarif national, le « web defacement » axé sur des modifications non autorisées de la page d'accueil d'un site web, ou encore le « spoofing » qui est une usurpation d'identité. " READ MORE

Source: Motherboard

Date: 7 Apr 2018

"Don't Mess With Our Elections": Vigilante Hackers Strike Russia, Iran

"On Friday, a group of hackers targeted computer infrastructure in Russia and Iran, impacting internet service providers, data centres, and in turn some websites. In addition to disabling the equipment, the hackers left a note on affected machines, according to screenshots and photographs shared on social media: "Don't mess with our elections," along with an image of an American flag. […] Cybersecurity firm Kaspersky said the attack was exploiting a vulnerability in a piece of software called Cisco Smart Install Client. Using computer search engine Shodan, Talos (which is part of Cisco) said in its own blog post on Thursday it found 168,000 systems potentially exposed by the software." READ MORE

Source: Sky News

Date: 5 Apr 2018

1.5bn sensitive files are exposed on the Internet, security researchers say

"More than 1.5 billion sensitive files - ranging from payslips to medical scans - are visible on the open internet, according to a new report. Security researchers have warned the documents are "freely available" to anyone with minimal technical knowhow, and 36% of the exposed files were located in the European Union. Confidential corporate data - including details of yet-to-be-released products - were also out in the open. In one case, a point of sale terminal was leaking data on customer transactions, times, places, and even partial credit card numbers." READ MORE

Source: Sydney Morning Herald

Date: 11 Apr 2018

Increasing cyber-crime attacks 'costing up to $1b a year' to Australian citizens

"Australians are being promised a stronger "cyber defence" agenda in Canberra to protect them from online crime that costs up to $1 billion a year, as key ministers warn of increasing attacks on essential infrastructure. The threats include privacy breaches to "harvest" the personal details of consumers as well as targeted strikes on essential services such as hospitals, according to details to be presented to a cybercrime summit this week. Home Affairs Minister P. Dutton warned of devastating threats to Australian infrastructure, revealing that Australian agencies helped bring down the Phantom Secure group of online criminals using encrypted communications." READ MORE

Source: Egypt Independent

Date: 12 Apr 2018

Egypt to punish ISP's refraining from blocking websites which 'threaten national security'

"Egypt's Parliamentary Committee of Communications and Information Technology approved recently Article 31 of the draft-law of the cyber-crime bill that stipulates punishing any internet service provider (ISP) which refrains from implementing website blocks issued by courts. According to state-run newspaper Al-Ahram, the article stipulates that that a penalty of no less than one year's imprisonment and a minimum fine of LE500,000 will be imposed on any ISP refraining from implementing a decision issued by the Criminal Court to block any of sites representing a 'threat to Egypt's national security'. […] Since May 2017, about 500 websites, including news and human rights sites, have been blocked to the Egyptian public. Blocked sites includes independent news website Mada Masr, the privately-owned Daily News Egypt, and Qatari-owned news agencies Al-Jazeera, El-Sharq, Al-Raya and Al-Watan, in addition to the US-based HuffPost Arabic." READ MORE

Source: The Straits Times

Date: 11 Apr 2018

Malaysia's anti-fake news legislation becomes law, is now enforceable

"Malaysia has gazetted the controversial Anti-Fake News Act 2018, meaning it has become law and is enforceable. Prime Minister Najib Razak said on Wednesday (April 11) that the Bill on anti-fake news has received assent from the Malaysian King and was gazetted on Wednesday, New Straits Times quoted him as saying. The Bill was fast-tracked in Parliament by the government last week although it was attacked by the opposition and political activists who feared it would be used to muzzle opinion that the ruling Barisan Nasional (BN) coalition disagreed with. There are also concerns that BN will use the law to stop criticisms against it in the ongoing election season. Datuk Seri Najib said the new law would not curtail the freedom of journalists. […] Germany passed its anti-fake news law in January with the authorities given the powers to fine social media giants up to €50 million (S$81.3 million) if they do not promptly remove illegal content from their sites. Other countries such as Singapore and the Philippines are mulling over anti-fake news laws too." READ MORE

Source: The Verge

Date: 8 Apr 2018

A broken submarine cable knocked a country off the internet for two days

"On March 30, the ACE Submarine cable cut out, dropping connectivity for much of West Africa. According to reports, the breach came off the coast of Mauritania, resulting in significant connectivity drops for at least ten neighboring countries. Mauritania itself was offline for nearly 48 hours before connectivity was partially restored. Other countries had enough terrestrial cable and satellite connections to route around the downed cable, but they still saw significant disruptions in internet access for most of the weekend." READ MORE

Latest reports

- ICANN, Data Protection/Privacy Issues Update: Soliciting Community Input on Article 29 Guidance, 13 Apr 2018
- Art. 29 Working Party, Guidance notes on how to ensure that WHOIS directories and services will be compliant with the GDPR, 11 Apr 2018
- National Cyber Security Center UK, The cyber threat to UK business 2017-2018 report, 11 Apr 2018
- RSIS, Cyber Deterrence in Singapore - Framework and Recommendations, 2 Apr 2018
- Article 19, Italy: Responding to 'hate speech', Country Report, April 2018
- AT Kearney, Cyber Security in ASEAN: An Urgent Call to Action, April 2018
- Serianu, Demystifying Africa's Cyber Security Poverty Line, Presented in April 2018

Upcoming events

- 16–19 April, Tirana, Albania – Case simulation exercise on cybercrime and financial investigations, iPROCEEDS
- April, Tirana, Albania – Advice on lessons learnt from case simulation exercise, iPROCEEDS
- 16–19 April, Santiago, Chile – Country assessment visit, GLACY+
- 18–19 April, Dublin, Ireland – Participation in Meeting of the Cybercrime Working Group at the Pompidou Group, Cybercrime@EAP 2018
- 18–20 April, Accra, Ghana – Integration of ECTEG materials in the training strategy for law enforcement officers, GLACY+
- 19–20 April, Podgorica, Montenegro – Pilot training session on introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (1st part), iPROCEEDS
- 20 April, Tbilisi, Georgia– Contribution to the International Festival of Cyber Security – IFC2018, Cybercrime@EAP 2018
- 23–25 April, Lisbon, Portugal – 1st EuroMed Conference on Digital Evidence, CyberSouth
- 24–27 April, Abuja, Nigeria – Country assessment visit, GLACY+
- 25–26 April, Yerevan, Armenia – Advisory Mission on 24/7 Points of Contact – Functions and Institutional Setup, Cybercrime@EAP 2018
- 30 April, Beirut, Lebanon – Planning meeting with CT MENA Project to prepare the Advisory Mission of Internal Security Forces in Lebanon, CyberSouth

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE