Cybercrime Digest

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

16-30 June 2017

Source: BTA

Date: 20 Jun 2017

Priorities of Bulgaria's EU Council Presidency unveiled to partners in Brussels

"Justice Minister Tsetska Tsacheva discussed the priorities of Bulgaria's Presidency of the EU Council in the first half of 2018. Tsacheva and EU Commissioner Dimitris Avramopoulos, who is responsible for Migration, Home Affairs and Citizenship, identified a need for unity and support in implementing policies for the protection of the EU's borders, the prevention of illegal migration, cyber security and the collection of e-evidence by the law enforcement and judicial authorities. They concurred on the need for speedy work during the Bulgarian Presidency of the EU Council on legislation on EU border protection, the interaction among the EU agencies in the area of security and encryption, the regulation on the exchange of data regarding the criminal records of third country nationals, and the collection of e-evidence." READ MORE

Source: Forbes

Date: 27 Jun 2017

Another Massive Ransomware Outbreak Is Going Global Fast

"Ukraine's government, National Bank, its transportation services and largest power companies are bearing the brunt of what appears to be a massive ransomware outbreak that's fast spreading across the world and hitting a significant number of critical infrastructure providers. […] The impact initially appeared to be most severe in Ukraine, with very few instances in the U.S., according to Kaspersky. The government organization managing the zone of the Chernobyl disaster fallout said it had to switch radiation monitoring services on industrial sites to manual as they had to shut down all Windows computers. Automated systems for the rest of the zone operated normally. The main Chernobyl plant website has also been closed." READ MORE

RELATED ARTICLES

Krebs on Security, 'Petya' Ransomware Outbreak Goes Global, 27 Jun 2017

Source: Department of Justice Philippines

Date: 27 June 2017

Enhancing regional and international cooperation in the Southeast Asian region

"The Philippine Department of Justice and the Council of Europe jointly organised a conference for countries in the Southeast Asian region to improve regional and international cooperation against cybercrime. ..."Governments have the obligation to protect the rights of individuals and to maintain the rule of law in cyberspace. Therefore, the capacities of criminal justice authorities to investigate cybercrime and secure electronic evidence need to be enhanced. At the same time, law enforcement powers must be subject to safeguards. This is also true for the ASEAN region", said Alexander Seger who heads the Cybercrime Division at the Council of Europe." READ MORE

RELATED ARTICLES

Council of Europe, Regional Conference materials, 27 Jun 2017

Source: Europol

Date: 16 Jun 2017

Police across Europe issue warning about the online coercion and extortion of children

"Often referred to as 'sextortion' or 'webcam blackmailing', the online coercion and extortion of children – a form of digital blackmail where sexual information or images are used to extort sexual material, sexual favours or money, has skyrocketed in the past years, but remains largely underreported. In a report released today by Europol, it is revealed that victims as young as 7 years old are being targeted online. When targeting a minor, offenders have two main motivations: (i) A sexual interest in children, where the objective of the extortive exchange is the procurement of sexual material (photos and/or videos) or a sexual encounter offline; (ii) An economic interest, where the objective is to gain financially from the extortion." READ MORE

Source: Digital Journal

Date: 22 Jun 2017

Germany expands surveillance of encrypted message services

"Amid the wave of jihadist attacks in Europe, German lawmakers voted in favour of the law designed "to reinforce the effectiveness of criminal procedures". German investigators will now be able to insert into users' cellphones and computers spy software (or a "Trojan horse") to access data in encrypted message services such as popular applications WhatsApp and Skype, including as part of criminal investigations." READ MORE

Source: Reuters

Date: 24 Jun 2017

UK Parliament hit by 'sustained and determined' cyber attack on MP emails

"Britain's parliament was hit by a "sustained and determined" cyber attack on Saturday designed to identify weak email passwords, just over a month after a ransomware worm crippled parts of the country's health service. The House of Commons said it was working with the National Cyber Security Centre to defend parliament's network and was confident it had protected all accounts and systems. "Earlier this morning we discovered unusual activity and evidence of an attempted cyber-attack on our computer network," an email sent by parliamentary authorities to those people affected said." READ MORE

Source: Council of Europe

Date: 16 Jun 2017

Strengthening Cybercrime Training Strategies for Law Enforcement Agencies

"The first in a series of workshops was held in Brussels on 15 and 16 June, which brought together 37 epresentatives of cybercrime units and police training academies from 20 countries to familiarize them with the ECTEG (European Cybercrime Training and Education Group) course materials and discuss national law enforcement training strategies and international best practices. Getting access to ECTEG materials will be facilitated by Council of Europe and further assistance provided to deliver these training courses at their national level." READ MORE

RELATED ARTICLES

Council of Europe, International Conference materials, 16 Jun 2017

Source: Daily MIrror

Date: 28 Jun 2017

Nigerian scam was busted by CID in Sri Lanka

"A group of 25 Nigerian and Ugandan nationals had been rounded up recently by the Criminal Investigation Department (CID) for swindling a sum of Rs.50 million from over 15 locals through fake Facebook posts. Police Media Spokesman SP Ruwan Gunasekara stated yesterday that these foreigners were arrested by the CID on charges of financial fraud." READ MORE

Source: Samoa Observer

Date: 25 Jun 2017

Top lawyers meet in Samoa, AG recommends ratification of the Budapest Convention

"Gender-based violence, environmental crime and cybercrime were among the issues discussed by the Pacific Islands Law Officers' Network (P.I.L.O.N). […] According to the Attorney General, the meeting discussed matters such as the M.O.U between Samoa, NZ and Australia, confirming that the P.I.L.O.N Secretariat will remain in Apia. "It also evaluated, confirmed and affirmed the on-going work of the three working groups for the areas of S.G.B. Violence, Environmental Crime and Cybercrime. The work of these groups encourages co-operation and assistance for regional and domestic changes to support on-going legal development. Cybercrime is chaired by the Kingdom of Tonga as led by their D.P.P and Acting AG Aminiasi Kefu, and after attending their seminar 22-25 May 2017, the AG of Samoa has recommended that government consider taking steps towards ratification of the Budapest Convention on Cybercrime." READ MORE

Source: Senado de la Republica, Estados Unidos Mexicanos

Date: 25 Jun 2017

Mexico, exhortan al Gobierno Federal adherirse al Convenio sobre Ciberdelincuencia

"A fin de fortalecer el marco jurídico en materia de ciberseguridad y reforzar la cooperación internacional para prevenir estos delitos, la Comisión Permanente exhortó a las dependencias del Gobierno Federal para que el Estado mexicano se adhiera y aplique las disposiciones del Convenio sobre Ciberdelincuencia, conocido como Convenio de Budapest, su protocolo adicional, así como al Convenio 108 del Consejo de Europa. El Convenio sobre la Ciberdelincuencia del Consejo de Europa, entró en vigor el 1° de julio de 2004 y constituye el primer tratado internacional sobre delitos cometidos a través de internet y de otros sistemas informáticos." READ MORE

Source: Entorno Inteligente

Date: 28 Jun 2017

Chile, 60 millones de potenciales ciberataques detectó red del gobierno en 2016

"Un segundo ciberataque de alcance global sacudió al planeta ayer, afectando a grandes empresas e incluso de los computadores de la central nuclear de Chernobyl, en Ucrania. […] Fue tal el impacto de Wannacry, que en Reino Unido afectó el funcionamiento de hospitales. En Chile, en cambio, no llegó a mayores según el balance que realizó el Ministerio del Interior y Seguridad Pública solicitado vía Ley de Transparencia por este medio. Existe una preocupación por este tema y en "avanzar en la comprensión, registro y caracterización del fenómeno asociado a incidentes", en este contexto destacan la reciente publicación de la Política Nacional de Ciberseguridad, el proyecto de ley de protección de datos personales, y la adhesión de Chile al convención del cibercrimen o convenio de Budapest." READ MORE

Source: Agence Ecofin

Date: 21 Jun 2017

Maurice sacrée championne de la cybersécurité en Afrique

"Avec son rang de sixième mondial, Maurice est le pays le mieux classé en Afrique, en 2017, selon l'indice de cybersécurité dans le monde de l'Union internationale des télécommunications. L'île s'est notablement illustrée dans les domaines juridique et technique, deux des piliers de l'enquête qui constitue un baromètre pour jauger le niveau d'engagement des Etats dans la lutte contre la cybercriminalité. […] Selon le document de l'organisation, le renforcement des capacités est un autre domaine où l'île Maurice a bien progressé." READ MORE

Source: Jeune Afrique

Date: 20 Jun 2017

Sénégal : la police emploie les grands moyens pour la cybersécurité

"D'ici fin juillet, une nouvelle division sera pleinement opérationnelle au sein de la police judiciaire sénégalaise. Chargée de lutter contre la cybercriminalité, elle sera aussi un nouvel outil important dans la lutte contre le terrorisme. […]Le champ d'action de cette « division cybersécurité » a aussi été élargi. Outre le traitement de la cybercriminalité « classique », elle aura pour autre objectif majeur de participer à la lutte contre le terrorisme. Dans la nouvelle équipe figurent des ingénieurs et des enquêteurs spécialisés, qui seront capables d'analyser différentes données numériques ou de « traiter » des outils saisis lors d'opérations de police, comme des téléphones portables, des ordinateurs, ou encore des disques durs." READ MORE

Source: MENAFN

Date: 22 Jun 2017

Afghanistan, President Signs Cybercrime Bill into Law

"President Ashraf Ghani has signed the bill on prevention of electronics crimes into law, the Ministry of Telecommunications and Information Technology said on Tuesday. Najib Nangyal, a spokesman for the IT ministry, told Pajhwok Afghan News the 27-article law had become part of the panel code after its approval by the president. Meanwhile, acting Telecom and IT minister Eng Syed Ahmad Shah Sadat said before there was no law to punish people for crimes they commit on the internet. 'Now when the law is approved, anyone who commits character assassination or misuses the social media, there are punishment codes and the accused can be tried. The law recommends fines and imprisonment up to 20 years as punishment, he said." READ MORE

Source: Reuters

Date: 19 Jun 2017

Thailand plans cyber network scrutiny, law to toughen online monitoring

"Thailand aims to buy software to strengthen the military government's ability to track online networks and monitor online activity while planning a cyber law that will expand powers to pry into private communications. The beefing up of powers over the online world come as authorities are increasingly targeting social media for violations of a law that makes it a crime to defame, insult or threaten the king, queen, heir to the throne or regent. The Digital Economy Ministry aims to spend 128.56 million baht ($3.8 million) on software including a "social network data analysis system" to monitor and map individuals and relationships between more than one million online users, according to a ministry document seen by Reuters." READ MORE

Source: ICANN

Date: 19 Jun 2017

ICANN Holds Its Second African Law Enforcement Capacity Building Workshop in South Africa

"Building on the success of the first workshop held in Nairobi, Kenya in January 2017, the Internet Corporation for Assigned Names and Numbers (ICANN) and Governmental Advisory Committee (GAC) Under Served Regions and Public Safety Working Groups announced their collaboration with the ZA Domain Name Authority on the second law enforcement agencies capacity development workshop from 23rd-24th June 2017 in Johannesburg, South Africa. The workshop aimed to continue to raise awareness amongst the joining African law enforcement community. A roundtable with ICANN community and industry focused on collaboration around security, stability and resiliency of the Internet" READ MORE

Source: Zambia Daily Mail

Date: 24 Jun 2017

Ongoing review of Electronic Communications legal framework in Zambia

"Minister of Transport and Communication, Brian Mushimba said with regard to the review of the existing legal framework, Government is in the process of unbundling the Electronic Communications and Transactions Act number 21 of 2009 into five distinct legislative Acts to be proposed to Parliament for enactment. He said the Acts include the Data Protection Bill, the e-Transactions and e-Commerce Bill, the Cyber Security Bill, and the Cybercrime Bill which is a penal law that will be used to prosecute cybercrime offences." READ MORE

Source: All Africa

Date: 22 Jun 2017

Namibia: Cybercrime Bill Flawed

"Unauthorised access to communications, warrant-less surveillance and interception and a lack of personal data and privacy protection are some of the main concerns voiced by civil society organisations over the draft provisions of the Electronic Transactions and Cybercrime Bill. The deadline to submit comments on the bill lapsed last Friday after it was put out for public comment by the Ministry of Information and Communication Technology (MICT) in mid-May, and some of the submissions expressed overwhelming concern that the draft law could infringe on constitutionally protected rights." READ MORE

Latest reports

- Council of Europe/Cybercrime Convention Committee, Sanctions and measures: implementation of Article 13 Budapest Convention, June 2017
- ENISA, Annual Incident Reports 2016 – Analysis of Article 13a annual incident reports in the telecom sector, June 2017
- APWG, Global Phishing Survey: Trends and Domain Name Use in 2016, June 2017
- FBI Internet Crime Complaint Center, Internet Crime Report 2016, June 2017
- ITU, Global Cyber Security Index 2017, June 2017
- Indian Strategic Studies, Transforming Election Cybersecurity, 21 Jun 2017
- China Digital Times, Cybersecurity Law in China: Reactions and Recent Enforcement, 23 Jun 2017
- The State of Security, Australia Cyber Security Strategy: SWOT Analysis, 26 Jun 2017

- Kaspersky, Ransomware in 2016-2017, 26 Jun 2017
- TechRepublic, 99.7% of web apps have at least one vulnerability, 26 Jun 2017

Upcoming events

- 3-6 July, Nuku'alofa, Tonga – Advisory mission on CERT capacities, digital forensics lab and public-private cooperation and Workshop on cybercrime reporting systems and collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, GLACY+
- 6-7 July, Mauritius – Advisory mission and workshop on cybercrime and cyber security policies and strategies, GLACY+
- 5-7 July, Minsk, Republic of Belarus – Seminar on CSIRT/CERT Regulations and Operational Environment, Cybercrime@EAP III
- 10-12 July, Tbilisi, Georgia – Advisory mission on 24/7 operations and regulations / consultative meeting, Cybercrime@EAP II
- 10-12 July, Mauritius – East African Regional Conference on Cybercrime and Electronic Evidence, in collaboration with the GPEN and with the participation of regional and international organizations and relevant countries from the Eastern African Region, GLACY+
- 10-13 July, Nuku'alofa, Tonga – Development of Cybercrime investigations, digital forensic capabilities combined with in-country workshops and advice on interagency cooperation and private public partnerships to fight cybercrime, GLACY+
- 14 July, Nuku'alofa, Tonga – Integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, 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