Cybercrime Digest

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

16-28 February 2017

Source: Europol

Date: 23 Feb 2017

Europol supports Poland and Romania in operation against online child sexual exploitation

"Europol have joined forces with Romanian Police and law enforcement authorities in Poland in a joint operation that has led to the arrest of a man suspected of online child sexual exploitation. The investigation uncovered that, between July 2012 and November 2015, the man was distributing child sexual abuse material. The victim was a boy of Polish nationality. On 16 February, Romanian police conducted a house search of the male in his late 30s in Bucharest. As a result four laptops, three hard drives, five memory sticks, 118 optical data storage devices and three memory cards were seized. At the request of the Romanian Prosecutor's Office, the suspect is currently detained and judicial proceedings are ongoing." READ MORE

Source: Irish Examiner

Date: 23 Feb 2017

Cyber criminals will face up to 10 years in jail in Ireland

"Sentences of up to 10 years will be available to the courts to deal with new offences to protect state bodies and businesses from cyber criminals and hackers. Legislation combating the area passed committee stage yesterday as part of an urgent drive across the European Union for strong laws and policing powers to deal with a surge in online attacks. Minister of State at the Department of Justice, David Stanton, yesterday said there was a "clear need" for international co-operation and harmonised laws "to counter this threat". He was speaking at the Oireachtas justice committee during its examination of the Criminal Justice (Offences Relating to Information Systems) Bill 2016, which implements a 2013 EU directive. Under the bill, it is an offence to intentionally access an information system without lawful authority, intentionally interfere with data or intercept the transmission of such data." READ MORE

Source: OAS

Date: 28 Feb 2017

Canada Commits Can$2.5 million to the OAS to Promote Cybersecurity Initiatives

"The Government of Canada and the Organization of American States (OAS) today signed an agreement by which Canada will contribute Can$2.5 million (US$1.88 mn) to OAS efforts "to enhance the capacity of OAS member states and other cybersecurity stakeholders to prevent and respond to threats posed by transnational cybercriminal activity and terrorism." READ MORE

Source: Le Huffington Post

Date: 15 Feb 2017

Le président français demande des "mesures spécifiques" contre les cyberattaques pendant la campagne présidentielle

"Alors que le sujet des cyberattaques visant la campagne électorale a regagné en intensité cette semaine avec les déclarations du camp Macron, François Hollande a demandé en Conseil de Défense que des "mesures spécifiques" soient prises pour protéger les élections, alors que Moscou est soupçonné d'avoir parasité le processus électoral américain. "Le Président de la République a demandé que lui soit présentées, lors du prochain Conseil, les mesures spécifiques de vigilance et de protection, y compris dans le domaine cyber, prises à l'occasion de la campagne électorale", indique l'Elysée dans un communiqué diffusé ce mercredi 15 février." READ MORE

Source: Balkan Insight

Date: 22 Feb 2017

Montenegro on Alert Over New Cyber Attacks

"The websites of the Montenegrin government and several state institutions, as well as some pro-government media, have been targeted with increasing numbers of cyberattacks in recent days, the government in Podgorica told BIRN. "The scope and diversity of the attacks and the fact that they are being undertaken on a professional level indicates that this was a synchronised action," the government said in a statement. […] The major new attack, which the government describes as more intense than the one in October, started on February 15 and peaked the following day, but continued over the weekend, the statement said." READ MORE

Source: Kosovo Police

Date: 22 Feb 2017

Supporting capacity building through iPROCEEDS Project

"Under the Joint Project of the European Union and the Council of Europe on targeting crime proceeds on the Internet in South-eastern Europe and Turkey – iPROCEEDS, two employees of Kosovo Police will attend the long-distance master programme MSc Forensic Computing and Cybercrime Investigation offered by the University College Dublin, Ireland. Participation in the programme is financed by iPROCEEDS project for duration of 24 months and will cover modules like Computer Forensics, Financial Investigation Techniques – Following the Money, Network Investigations, Mobile Devices Investigation, Live Data Forensics, VoIP and Wireless Investigations and others. Learning will take place through a mix of lectures, hands-on labs, case studies, reading, small group and individual exercises, tool demonstrations and in depth-discussions." READ MORE

Source: Lexology

Date: 21 Feb 2017

Ukraine: new cyber security protection measures

"On 13 February 2017 the President approved the National Security and Defence Council's decision on securing Ukraine against evolving cyber threats (the "NSDC Decision"). […]. The main cyber security measures envisaged by the NSDC Decision include the following: The Cabinet of Ministers shall propose draft laws to Parliament to implement the Convention on Cybercrime introducing, among others: the ability of the law-enforcement bodies to issue mandatory orders to electronic data owners for the immediate recording and storing of electronic data necessary to investigate crimes for a period from 90 days to 3 years; an obligation for telecom operators and providers to provide all data necessary to identify service providers and data routes to the law enforcement bodies, as per their request; the possibility to block informational resources by court decision; and an effective legal mechanism for the use of electronic evidence in criminal court proceedings." READ MORE

Source: Newsday Georgia

Date: 27 Feb 2017

EU tackling cybercrime in Georgia

"The Council of Europe (CoE) is collaborating with the High School of Justice of Georgia to organise a two-day training session for Georgian judges on the effective review of cybercrimes on 25-26 February in Tbilisi. The training is part of the joint EU/CoE project "Protecting Internet Freedom through Legislation and Arrangements for Multi-stakeholder Dialogue". CoE experts will review both national and international legislation including the Budapest convention on cybercrimes and the relevant national normative acts as well as standards set by the leading EU cases. This series of training sessions involving cybercrime experts and four Georgian judge trainers will enable the High School of Justice of Georgia to further carry out the in-service trainings provided by Georgian judges who have already trained." READ MORE

Source: Business Day

Public-private partnerships are key in fight against cybercrime in South Africa, MPs told

Date: 28 Feb 2017

"The government needs to promote public-private partnerships in order to counter cybersecurity breaches and incidents, Parliament heard on Tuesday. Officials from the Department of Telecommunications and Postal Services briefed MPs on efforts to boost SA's security arsenal to thwart cyber attacks. Cybercrime is now seen as one of the biggest threats to countries' critical information infrastructure and socioeconomic development. In SA, cybercrime is now the fourth-most reported economic crime, according to the findings of PwC's 2016 Global Economic Crime Survey. The South African Banking Risk Information Centre (Sabric) estimates that South Africans lose more than R2.2bn to internet fraud and phishing attacks annually." READ MORE

Source: Diario Judicial

"Necesitamos legislar sobre medidas para la obtención de evidencia digital"

Date: 25 Feb 2017

"En diálogo con Diario Judicial, abgado especialista en Derecho Penal y en delitos informáticos, Marcos Salt, celebró la voluntad de Argentina de adherirse al Convenio sobre Ciberdelincuencia, conocido como Convención de Budapest, y le enseñó a este medio las deficiencias que tiene el sistema procesal local a la hora de regular la obtención de pruebas en el entorno digital. […] "Marca una continuidad política del Estado Argentino en materia de combate de delitos informáticos y obtención de evidencia digital. Hace mucho tiempo que Argentina manifestó su voluntad de adherirse, pero en su momento no se hizo. Cuando empieza a discutirse cómo obtener la evidencia digital, cuando empieza a ser ya un problema a nivel internacional porque está globalizado, Argentina tiene que tomar la decisión respecto de cómo lo hace. Esta Convención, pese a estar hecha por el Consejo europeo, tiene características especiales, como por ejemplo que está "abierta" al mundo, porque se adhirieron países como Estados Unidos, Japón, Canadá, Israel, y dentro de la región se adhieran Chile, Republica Dominicana y Panamá. Con lo cual es el único convenio internacional sobre delitos informáticos y obtención de evidencia digital, con cooperación internacional específica en este último aspecto." READ MORE

Source: The Gleaner Jamaica

Belize Government looking at legislation to tackle misuse of social media

Date: 25 Feb 2017

"The Belize government is moving to clamp down on the misuse of the social media and is establishing a taskforce to look at the issue of cyber laws, Solicitor General, Nigel Hawke has said. "We've just discussed that there's a committee set up that is looking at the issue of cybercrime legislation but it's at the stage where it's just a number of multi-sectoral groups which have been discussing the issue with the view of coming up with a final policy position to take to Cabinet for approval," he said. "At some stage there will be some cybercrime bill or cyber security bill. That is the hope, but it's still on the horizon," he said, adding that it is hoped that it may take another two or three months before a proposal or a policy is placed before Cabinet." READ MORE

Source: Jamaica Observer

Date: 18 Feb 2017

Regional leaders end successful summit in Guyana

"Caribbean Community (CARICOM) leaders have ended a two-day summit adopting decisions that they said are important to moving the 15-member regional integration movement "towards its objects". CARICOM chairman and host, President David Granger told that the leaders had also reflected on the importance of the 'CARICOM brand', and the pride that we have in our citizenship, citizenry and membership. […] "We will be seeking to take full advantage of opportunities for capacity-building to address existing and emerging threats, including those related to cyber security and cybercrime, crime prevention and drug demand reduction." READ MORE

RELATED ARTICLES

CARICOM, President's Statement at the Conclusion of the 28th Intersessional Meeting of the Conference of Heads of Government, 17 February 2017

Source: Bleeping Computer

Date: 24 Feb 2017

World's Largest Spam Botnet Adds DDoS Feature

"Necurs, the world's largest spam botnet with nearly 5 million infected bots, of which one million active each day, has added a new module that can be used for launching DDoS attacks. Like most of today's top-tier malware families, Necurs' functionality is broken down across several modules that are loaded on infected computers in real-time, only when needed." READ MORE

Source: The Economic Times

Date: 22 Feb 2017

India's cyberspace intelligence agency to be functional from June

"In wake of the unprecedented rise in the digital transactions in the country, the government is fast-tracking its efforts to build a robust cyber security ecosystem. The country's apex cyberspace intelligence agency, the National Cybersecurity Coordination Centre (NCCC), will become functional in June this year while sector specific CERTs for industries such as power, communications etc, will also be created, Ravi Shankar Prasad, Union Minister for Electronics and IT said." READ MORE

Source: Silicon

Date: 28 Feb 2017

Data stolen from Singapore military in 'carefully planned' cyber attack

"Singapore's Ministry of Defence, Mindef, said basic personal information on 850 national servicemen and staff were stolen from an Internet-facing network in what it called a "targeted and carefully planned" attack. The individuals' national ID numbers, telephone numbers and dates of birth were stolen from a system called I-net which provides staff with Internet access for personal communications and viewing the web on thousands of dedicated terminals within Mindef's premises, as well as armed forces camps and premises. I-net holds no classified information and is not linked to the ministry's more sensitive internal systems, which have no connection to the Internet. The ministry said this was the first time I-net has been breached.." READ MORE

Source: Ministry of Foreign Affairs of Japan

Date: 24 Feb 2017

The 2nd ASEAN-Japan Cybercrime Dialogue

"On the 1st and 2nd of March, the 2nd ASEAN-Japan Cybercrime Dialogue will be held in Kuala Lumpur, Malaysia. This Dialogue will be co-chaired by Ms. Yukiko OKANO, Minister-Counsellor / Deputy Chief of Mission, of Japan to ASEAN; and Mr. Mohd Azlan Razali, Undersecretary, International Division, Ministry of Home Affairs, Malaysia. The Dialogue will be attended by officials from Japan, all the ASEAN Member States and the ASEAN Secretariat. This Dialogue was inaugurated in 2014 as a follow-up to the commitment made at the ASEAN-Japan Commemorative Summit in December 2013. The Dialogue is held to confirm the importance of Convention of Cybercrime (Budapest Convention) with the countries of ASEAN and discuss ASEAN-Japan cooperation on cybercrime, such as promotion of information-sharing on trends and lessons learned to combat cybercrime, promotion of international cooperation on cybercrime, capacity building to fight against cybercrime, and the direction of concrete activities using Japan-ASEAN Integration Fund (JAIF)." READ MORE

Latest reports

- Foundation for the Defense of Democracies, Framework and Terminology for Understanding Cyber-Enabled Economic Warfare, 22 Feb 2017
- World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards, February 2017
- Bruce Schneier, SHA-1 Collision Found, 23 Feb 2017
- Anti-Phishing Working Group, 2016 Exceeds All Records in Numbers of Phishing Attacks, February 2017
- Kaspersky, Malware mobiles : 8,5 millions d'installations malveillantes ont été détectées en 2016, février 2017

Upcoming events

- 6-9 March, Yerevan, Armenia – Training of investigators, prosecutors and judiciary in international cooperation on electronic evidence/multinational providers cooperation, EAP II/III
- 13-14 March, Podgorica, Montenegro – Regional workshop on introductory training module on cybercrime and financial investigations for cybercrime, financial investigation units, FIUs and specialised judges and prosecutors, iPROCEEDS
- 13-16 March, Baku, Azerbaijan – Training of investigators, prosecutors and judiciary in international cooperation on electronic evidence/multinational providers cooperation, EAP II/III
- 13-17 March, Colombo, Sri Lanka – Development of Cybercrime investigations, digital forensic capabilities (INTERPOL) combined with in-country workshops and advice on interagency cooperation (INTERPOL) and private public partnerships to fight cybercrime (INTERPOL), GLACY+
- 13-17 March, Dakar, Senegal – Support regional judicial ToT on cybercrime an EE, 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

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE