Cybercrime Digest

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

16-31 May 2017

Source: Nuku'alofa Times

Date: 23 May 2017

The Pacific Response to Cybercrime: effective Tools and Good Practices

"Opening the Pacific Island Law Officer's Network Cybercrime Workshop at the Tanoa Dateline International Hotel this morning, Tonga's Deputy Prime Minister Hon Siaosi Sovaleni said that many of the Pacific Island States face a threefold challenge when it comes to dealing with cybercrime and electronic evidence: (a) putting in place a comprehensive legislative framework in line with international standards, (b) improving capacities and know-how within the criminal justice sector to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence, and (c) engage in efficient international cooperation. He said the conference is a great opportunity for countries to work together on finding solutions as no country can face the cybercrime challenges alone." Senior officials from 13 Pacific island countries participated in the event, organized by PILON and supported by Council of Europe. READ MORE

RELATED ARTICLES

Tonga Ministry of Information & Communication, Pacific Islands Law Officers' Network cybercrime Workshop 23 – 25 May 2017, Nuku'alofa, Kingdom of Tonga, 24 May 2017

Source: Europol

Date: 18 May 2017

27 arrested in successful hit against ATM black box attacks in Europe

"The efforts of a number of EU Member States and Norway, supported by Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT), culminated in the arrest of 27 individuals linked with so-called ATM "Black Box" attacks across Europe. Perpetrators responsible for this new and sophisticated method of ATM jackpotting were identified in a number of countries over different periods of time in 2016 and 2017. There were arrests in Czech Republic (3), Estonia (4), France (11), the Netherlands (2), Romania (2), Spain (2) and Norway (3)." READ MORE

RELATED ARTICLES

EAST, ATM Black Box Attacks spread across Europe, 11 Apr 2017

Source: A.M. Costa Rica

Date: 22 May 2017

Legislators approve the Convention on Cybercrime in Costa Rica

"The Costa Rican legislature gave the second approval towards ratifying the Budapest Convention, according to a statement made by the science and technology ministry Friday afternoon. […] The Ministerio de Ciencia, Tecnología y Telecomunicaciones praised the legislative approval of the ratification. The ministry said that this would allow authorities to receive access to procedures, tests and collaborative initiatives around the world to detect cybercriminals. […] Costa Rica places seventh in the number of cyber attacks registered in Latin America, the ministry said." READ MORE

Source: Government of The Netherlands

Date: 19 May 2017

Dutch Foreign Minister calls on Turkey to follow the recommendations of the Council of Europe

"[…] The minister also spoke about the Convention on Cybercrime of the Council of Europe and encouraged countries that are not yet party to it to sign on as soon as possible. The reason for this urgency was the WannaCry ransomware virus, which last week affected organisations and individuals all over the world. 'Crime and terrorism are increasingly becoming cross-border problems, especially in the digital domain,' Mr Koenders said. 'The rapid spread of WannaCry ransomware made this painfully clear last weekend. Our priorities should be building users' resilience, thwarting cyberattacks, and finding and prosecuting the perpetrators. This can only be done if international cooperation between investigative agencies is organised effectively.' " READ MORE

Source: Irish Government News Service

Date: 18 May 2017

Irish legislation to deal with cybercrime completes its passage through the Houses of the Oireachtas

"The first piece of Irish legislation dedicated specifically to dealing with cybercrime today completed its passage through the Houses of the Oireachtas, where it received general, cross-party support. The Criminal Justice (Offences Relating to Information Systems) Bill aims to safeguard information systems and the data that they contain. The legislation creates new offences relating to: (i) unauthorised accessing of information systems; (ii) unauthorised interference with information systems or data on such systems; (iii) unauthorised interception of transmission of data to or from information systems, and (iv) the use of tools, such as computer programmes, passwords or devices, to facilitate the commission of these offences relating to information systems. " READ MORE

Source: Xinhua Net

Date: 16 May 2017

Kenya to fast track enactment of law to protect country from cyber attacks

"Kenya is fast-tracking the enactment of a law that will protect the country from cyber attacks, a senior government official said on Tuesday. Ministry of Information, Communications and Technology (ICT) Cabinet Secretary Joe Mucheru told journalists in Nairobi that the Cabinet has already approved and forwarded to Parliament for debate the Computer and Cyber Crimes Bill that seeks to increase penalties for cybercrime and related corporate espionage. […] The Bill draws heavily from best practices elsewhere including the Budapest Convention on Cybercrime that was passed by the Council of Europe in 2001." READ MORE

Source: Hindustan Times

Date: 21 May 2017

India, Israel to enlarge web of ties, institutionalise cyber security dialogue

"With national cyber security coordinator in the Prime Minister's Office Dr Gulshan Rai bound for Tel Aviv this week, India and Israel are all set to institutionalise cyber security cooperation in the run-up to Prime Minister Narendra Modi's maiden visit to Jerusalem in July. […] India and Israel would like to exchange notes on protecting national databases from malware and hackers. The two sides are preparing to set up a dialogue or a joint working group where cyber-experts from both sides could exchange information or technologies for mutual benefit." READ MORE

Source: Security Week

Date: 30 May 2017

China to Launch Cybersecurity Law Despite Concerns

"China will implement a controversial cybersecurity law Thursday despite concerns from foreign firms worried about its impact on their ability to do business in the world's second largest economy. Passed last November, the law is largely aimed at protecting China's networks and private user information at a time when the recent WannaCry ransomware attack showed any country can be vulnerable to cyber threats. But companies have pleaded with the government to delay the legislation's implementation amid concerns about unclear provisions and how the law would affect personal information and cloud computing." READ MORE

Source: Free Malaysia Today

Date: 29 May 2017

Malware a growing threat in Malaysia, says study

"Malaysia ranks fifth in volume of malware detected among countries in the Asia Pacific region, a new study says. Although Malaysia ranks in the top 20 globally in terms of total malware detections, it performs the best among the emerging countries with a malware detection rate that is two to three times lower. According to the Asia Pacific State of Malware report 2017, emerging markets in Asia Pacific such as Indonesia, India, the Philippines, Thailand and Malaysia are more likely to be harmed by malware infections than others." READ MORE

Source: Papua New Guinea Post-Courier

Date: 18 May 2017

Cyber Security Law yet to be enforced in Papua New Guinea

"Capacity and capability are needed to effectively enforce the cybercrime law, says Communication and Information secretary Paulius Korni. Mr Korni said the Cybercrime Code Act is now in force. However, responsible institutions are lacking with the necessary skills, knowledge and tools to enforce the law. He said that the government has also been alerted on the recent report by the international media on hackers being able to hack into the health systems of multiple countries, including Great Britain and Russia, and have jeopardised the critical life-supporting ICT systems." READ MORE

Source: Deep Dot Web

Date: 24 May 2017

Darknet Vendor Lists One Billion Anti-Public Accounts

"On May 5, the creator of the famed "Have I Been Pwned?" breach alert system, Troy Hunt, announced that he loaded "over 1 billion breached accounts into HIBP." At the date of his blog post, HIBP hosted 2.7 billion breached accounts from numerous breaches. "There's a lot more there now," he explained, referring to a massive number of breached accounts—currently for sale as anti-public username lists." READ MORE

Source: Internet Society

Date: 30 May 2017

Internet infrastructure security guidelines for Africa

"In 2014, African Union members adopted the African Union Convention on Cyber Security and Personal Data Protection. To facilitate implementation of the Convention, the African Union Commission asked the Internet Society to jointly develop Internet Infrastructure Security Guidelines for Africa. […] The Guidelines emphasize the importance of the multistakeholder model and a collaborative security approach in protecting Internet infrastructure. The Guidelines put forward four essential principles of Internet infrastructure security: Awareness, Responsibility, Cooperation, and adherence to Fundamental Rights and Internet Properties." READ MORE

Source: L'Evénement Précis

Date: 18 May 2017

Les cyberattaques dans la cybercriminalité en Afrique

"Les cyberattaques pures ne représentent qu'une infime proportion des actes de cybercriminalité enregistrés en Afrique. « Au Sénégal par exemple, 90% des actes de cybercriminalité sont des cyberescroqueries et 10% seulement sont des cyberattaques pures», témoigne Issa Diack, commandant de la Section de recherche de la gendarmerie nationale du Sénégal. Ce tableau correspond à peu près à celui qu'on rencontre au Bénin, selon les indications du commissaire Nicaise Dangnibo, chef de l'Office central de répression de la cybercriminalité. «Au Bénin, dit-il, la cyberescroquerie sous toutes ses formes (arnaque aux sentiments, chantage à la vidéo, faux prêts, faux contrats de bail, fausses offres d'emplois, fausses bourses d'études, etc.) représente 94% des actes de cybercriminalité, contre 6% de cyberattaques pures»" READ MORE

Source: Afrique La Tribune

Date: 27 May 2017

Nigeria : les Etats-Unis à la rescousse pour contrer la cybercriminalité

"Afin de délester le Nigeria des maux qui grèvent son économie, les Etats-Unis viennent d'annoncer officiellement leur intention de collaborer avec les autorités nigériennes dans leur lutte contre la cyber-criminalité et les crimes financiers. Stuart Symington, l'ambassadeur américain en poste à Abuja, a en effet révélé que les deux pays s'associent désormais contre la cybercriminalité et les fraudes financières. «Les Etats-Unis vont collaborer avec le gouvernement nigérian dans le cadre de la lutte contre la fraude financière, le blanchiment, la cybercriminalité, les crimes transfrontaliers dont le trafic de stupéfiants, humain, et le braconnage», a déclaré le diplomate." READ MORE

Source: Nampa

Date: 24 May 2017

Cyber Crime Bill tabling reversed for consultation in Namibia

"The draft of the Electronic Transactions and Cyber Crime Bill has been reversed from tabling in the National Assembly to allow for public involvement and scrutiny through consultation. Permanent Secretary (PS) in the Ministry of Information and Communication Technology (MICT), Mbeuta Ua-Ndjarakana said at a media conference on Wednesday that the public is therefore requested to get hold of the Bill for inputs and comments before 16 June." READ MORE

Source: Tic Mag

Date: 30 May 2017

Cybercriminalité : Le Togo envisage de se doter d'une cyberpolice

"Face à la menace, le gouvernement togolais envisage de se doter d'une cyberpolice. Il s'agira selon Pius Kokouvi Agbétomey, le ministre togolais de la Justice d'une police spécialisée sur des questions de cybercriminalité, qui dispose des moyens appropriés à la hauteur de la menace. Dans ce sillage, le gouvernement togolais a commencé à former dès le 29 mai 2017 des officiers de police judiciaire aux nouvelles techniques d'investigations et de recherches par le Centre de Formation des Professionnels de Justice. Sur le long terme, ces officiers devraient compléter leur formation dans des pays en pointe de la lutte contre la cybercriminalité et se doter des outils modernes que possèdent déjà les cybercriminels pour perpétrer leurs forfaits." READ MORE

Latest reports

- Council of the European Union, Access to electronic evidence - findings from the expert process and suggested way forward, 22 May 2017
- African Union Commission, GFCE, Symantec, Cyber Crime & Cyber Security Trends in Africa, October 2016, presented in May 2017
- Institute for Advanced Legal Studies, Electronic Evidence – Fourth Edition, 4 May 2017
- ICMEC, Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation, May 2017
- Privacy International, Cyber Security in the Global South, May 2017
- O. Catakoglu, M. Balduzzi, D. Balzarotti, Attacks Landscape in the Dark Side of the Web, May 2017
- Kaspersky, Spam and phishing in Q1 2017, 2 May 2017

Upcoming events

- 5 June, Turin, Italy – Participation in the UNICRI Specialized Training on International Criminal Law and Global Threats to Peace and Security, GLACY+
- 5-7 June, Tallinn, Estonia – Steering committee meeting and participation at EuroDIG 2017 conference, Cybercrime@EAP II / Cybercrime@EAP III
- 5-8 June, Madrid, Spain – Participation in the INTERPOL Eurasian Working Group on Cybercrime for Heads of Units and in the Operational side-meeting on Business Email Compromise, GLACY+
- 7-9 June, Strasbourg, France – Participation in the 17th plenary of the T-CY, GLACY+ / iPROCEEDS / Cybercrime@EAP II
- 12-13 June, Luxemburg – International workshop for cybercrime and specialised units on techniques to search, seize and confiscate proceeds from crime online, iPROCEEDS
- 13-14 June, Podgorica, Montenegro – Country visit to assess the guidelines to prevent and detect/identify online crime proceeds, iPROCEEDS
- 14 June, Skopje, "The former Yugoslav Republic of Macedonia" – Meeting to support/establish existing public/private initiatives, iPROCEEDS
- 15-16 June, Skopje, "The former Yugoslav Republic of Macedonia" – Country visit to assess the guidelines to prevent and detect/identify online crime proceeds, iPROCEEDS
- 15-16 June, Brussels, Belgium – International workshop on cybercrime training strategies for law enforcement agencies and access to ECTEG materials in cooperation with INTERPOL and ECTEG, GLACY+ / iPROCEEDS / Cybercrime@EAPIII

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