Cybercrime Digest

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

16-31 January 2018

Source: The Indian Express

Date: 18 Jan 2018

India, Home Ministry pitches for Budapest Convention on cyber security

"Making a strong pitch to sign the Budapest Convention on cyber crime, the Ministry of Home Affairs flagged the need for international cooperation to check cyber crime, radicalisation and boost data security. Officials said India was reconsidering its position on becoming a member of the Budapest Convention because of the surge in cyber crime, especially after a push for digital India. […] Home Ministry officials told The Indian Express that a final decision on signing the Convention will be taken after consulting other stakeholders, such as the Ministry of External Affairs and the Ministry of Communication and Information Technology." READ MORE

Source: White House

Date: 16 Jan 2018

United States and Kazakhstan: An Enhanced Strategic Partnership for the 21st Century

"The two leaders pledged to deepen bilateral defense and security relationships, noting their intent to conclude several agreements that enhance cooperation, interoperability, access, and logistical routes in support of regional security. […] The presidents committed to explore Kazakhstan's interest in joining the Cybercrime Convention, which would provide a framework for global cooperation against threats to e-commerce and crimes committed over the internet. Participation in these kinds of multilateral agreements further strengthens law enforcement cooperation and information sharing to combat international terrorism and violent extremism." READ MORE

Source: NITA Uganda

Date: 19 Jan 2018

Uganda, Ministry of ICT & National Guidance hosts the Council of Europe on the Budapest Convention

"The Government of Uganda through the European Union and Council of Europe has obtained support to assist Uganda harmonize legislation on Cybercrime and electronic evidence towards Ratification of the Budapest Convention on Cyber Crime. The Budapest Convention on Cybercrime is an international treaty that seeks to address Internet and Computer Crime by harmonizing national laws on cybercrime, improving national capabilities for investigating such crimes, and increasing cooperation on investigations." READ MORE

Source: LSM LV

Date: 16 Jan 2018

DDoS attack hits Latvia's national 'e-health' system

"On January 16 the National Health Service IT system and the 'e-health' system used by doctors to write prescriptions and sick leaves came under cyber attack, the Health Ministry told LSM's Latvian-language service. […] "An investigation has been started. It is clear it was a planned attack, a distributed attack, as experts call it. It was carried out from several countries, or rather computer systems in several countries. [Computers] from both EU and non-EU countries were involved, more than 20 in total," said Health Ministry State Secretary Aivars Lapiņš at a press conference." READ MORE

Source: Romania Insider

Romanian criminal group investigated for illegally selling EUR 12 mln worth of drugs online

Date: 25 Jan 2018

"Prosecutors from the Directorate for Organized Crime and Terrorism (DIICOT) and police officers carried out dozens of home searches on Thursday, January 25, in a case targeting a local organized crime group that allegedly sold online some EUR 12 million worth of drugs such as Xanax or Codeine, with the help of pharmacists. […] They were taking orders from clients online, using so-called pharmacy websites, through a call center based in Cluj-Napoca. The group members were simulating medical checks, making their clients believe that they were being consulted by a real physician, and thus convincing them to place the orders. To get the drugs, the customers were asked to pay the money in advance, through money transfer services or in Bitcoin." READ MORE

Source: The Guardian

Major cyber-attack on UK a matter of 'when, not if' – security chief

Date: 23 Jan 2018

"The head of the UK's National Cyber Security Centre has warned that a major cyber-attack on the UK is a matter of "when, not if", raising the prospect of devastating disruption to British elections and critical infrastructure. In remarks underlining newly released figures showing the number of cyber-attacks on the UK in the last 15 months, Ciaran Martin said the UK had been fortunate to avoid a so-called category one (C1) attack, broadly defined as an attack that might cripple infrastructure such as energy supplies and the financial services sector. The US, France and other parts of Europe have already faced such attacks. Interference in elections would also constitute a C1 attack, as would a deliberately provocative move by a hostile state." READ MORE

Source: The National

Almost 800 cybercrime cases handled by Abu Dhabi police last year

Date: 22 Jan 2018

"Abu Dhabi police investigated 774 cybercrime cases in 2017, of which 206 were categorised as blackmail. Brig Tariq Al Ghoul, Director of the Directorate of Criminal Investigation and Investigation, said Abu Dhabi police were taking extra care to combat cybercrimes with innovative methods and technologies. He also called upon the public to safely use the internet, to avoid fraud and blackmail and becoming involved in criminal cases. He also cautioned about spamming and fraud, and avoiding falling prey to cybercrimes along with the necessity of being careful with what is published on websites or social media, to preserve the confidentiality of individual's data and privacy." READ MORE

Source: The Express Tribune

Pakistan, threats through electronic communication criminalised

Date: 17 Jan 2018

"The federal cabinet on Tuesday approved criminalising certain offences under cybercrime and its related laws that were previously proceeded against under the Pakistan Penal Code (PPC). Those include hurling threats and harassment through any form of electronic communication (in addition to the internet). The approval was granted during the weekly cabinet meeting presided over by Prime Minister Shahid Khaqan Abbasi." READ MORE

Source: DhakaTribune

Date: 31 Jan 2018

Bangladesh, only 5% conviction rate in cyber crime cases over 5 years

"There have been only 16 successful convictions across 12 of the 236 cases heard before the tribunal since its inception in February 2013. The repeated failure of the prosecution and law enforcement agencies to prove allegations of cyber crime has resulted in a paltry conviction rate of only 5% over the past five years, according to the records of the Cyber Tribunal (Bangladesh) in Dhaka. There have been only 16 successful convictions across 12 of the 236 cases heard before the tribunal since its inception in February 2013. In 129 of the other cyber crime cases, the accused were cleared of all charges in the final report submitted before the tribunal by police. The tribunal discharged the accused in a further 59 cases without taking charges into cognizance, while the defendants in 36 cases were acquitted as the prosecution failed to prove the charges during the trial." READ MORE

Source: IT Web Africa

Date: 22 Jan 2018

Communications Authority warns Kenyans on emerging cyber crime

"The Communications Authority of Kenya (CA), through the National Computer Incident Response Team Coordination Center (National KE-CIRT/CC), has issued a cybercrime warning and an advisory on supply chain risks in using third-party software. According to CA, the advisory aims help ICT users make informed and risk-free decisions on their product choices by engaging cybersecurity experts. The regulatory body says cyber criminals are now mostly using third-party software to deliver threats to unsuspecting users, in an attempt to compromise their personal data. […] In a recent cyber crime incident, hackers breached systems belonging to the National Bank of Kenya and made away with Ksh 29 million. The bank recently confirmed the incident on 17 January, through a statement on its twitter handle: "The amount of attempted fraud is about Ksh 29 million and we are confident we will recover most of that money." READ MORE

RELATED ARTICLES

Standard Digital, Hundreds of millions of cyber-attacks take place every year in Africa, 17 Jan 2018

Source: Lusaka Times

Date: 27 Jan 2018

Zambia Government to introduce laws against social media misuse

"Transport and Communications Minister Brain Mushimba has clarified and reassured the public that government will not shut down social media but regulate its use. Mr. Mushimba said he will be taking three bills to parliament that supports productive use of internet and social media. He said the bills will be cyber security and cyber-crime bill, e-commerce bill and data protection bill. He said government was concerned with the ongoing abuse of the internet which manifested in cyber bullying, posting of fake news, fraud and the creation of fake accounts on social media." READ MORE

RELATED ARTICLES

Lusaka Times, Zambia ICT Authority says it has put measures in place to fight cyber-crime, 25 Jan 2018

Source: Computer Weekly

Date: 31 Jan 2018

Navigating ASEAN's patchy cyber security landscape

"Singapore's upcoming Cybersecurity Bill – slated to become law this year – is crafted to ensure that organisations in critical sectors such as financial systems are able to demonstrate a level of cyber security preparedness. Also critical is the need to disclose and share with the commissioner of cyber security full details of any cyber security breaches. […] It is difficult, if not impossible, to make direct comparisons as to which countries have 'better' or 'more comprehensive' strategy. The other markets in the region have poor disclosure laws – consequently many breaches go unpublicised, leaving many organisations to believe a country is 'safe' from attack, when in fact the breaches are many and are simply unknown to the public at large and possibly even the government. Other countries such as Malaysia, Thailand and Vietnam have also drafted cyber security bills, while cyber crime laws have been passed in Singapore, Malaysia, Thailand, the Philippines and Brunei. Five of the six most developed countries in ASEAN have also enacted data protection and privacy laws." READ MORE

Source: Zimbabwe Independent

Date: 26 Jan 2018

Zimbabwe, Cybersecurity Bill raises concerns of the Media Institute of Southern Africa

"The Zimbabwe chapter of the Media Institute of Southern Africa has raised concerns over sections of the Cybercrime and Cybersecurity Bill which allow investigating authorities to seize computer devices and mobile phones during investigations, even if the equipment is not directly involved in the criminal activity being investigated. Although the Bill has been amended several times, it has largely been seen as an instrument for government to tighten its grip over the control of cyberspace while spying on citizens. The Bill is yet to be passed by parliament." READ MORE

Source: Xinhua Net

Date: 20 Jan 2018

Rwandan banks highly vulnerable to cyber attacks: central bank

"Governor of the National Bank of Rwanda on Friday called on Rwandan financial institutions to be wary of looming cyber attacks in the region, particularly in banking institutions where defences are inadequate. John Rwangombwa made the call while speaking at a national forum on cyber and financial crimes." READ MORE

Source: La Voz

Date: 26 Jan 2018

El ciberespacio, territorio sin fronteras para el delito

"El ciberespacio ha tenido un desarrollo sin igual en las últimas dos décadas, pero también ha servido para que en su seno hayan crecido las modalidades delictivas más insospechadas. La capacidad de daño, estafa o robo, por citar algunos perjuicios, parece ser ilimitada desde el mundo virtual. […] Hay que cambiar la idea de que el ciberespacio es un lugar físico. Hay una interconexión de equipos informáticos que necesita una regulación propia, fuera del mundo físico, porque la característica de este lugar es que altera la relación eje espacio-temporal que rige el mundo físico. Se trata de un espacio en el que no hay fronteras, no hay aduana, no hay pasaportes; se puede pasar de un país a otro en instantes. Hay que regular y empezar de cero, a través del derecho informático. […] Todo está subordinado al Convenio de Budapest, el marco de ciberdelitos más grande del mundo." READ MORE

Latest reports

- Council of the European Union, EU priorities for cooperation with the Council of Europe in 2018-2019, 22 Jan 2018
- European Commission, Communication from the Commission to the European Parliament, the European Council and the Council – Thirteenth progress report towards an effective and genuine Security Union, 24 Jan 2018
- ENISA, Looking into the crystal ball: A report on emerging technologies and security challenges, 31 Jan 2018
- Europol and ENISA, Common Taxonomy for Law Enforcement and CSIRTs, December 2017
- ICANN, Data Protection/Privacy Update: Status of Compliance Model Selection for the new WHOIS, 25 Jan 2018
- World Economic Forum, The Global Risks Report 2018, January 2018
- Office for National Statistics UK, Overview of fraud and computer misuse statistics for England and Wales, 25 Jan 2018
- CLUSIF, Panorama de la Cybercriminalité – Année 2017, 25 Jan 2018
- Norton, Cyber Security Insights Report 2017 Global Results, January 2018
- RAND, Estimating the Global Cost of Cyber Risk, 15 Jan 2018

Upcoming events

- 5 – 7 February, Lisbon, Portugal – Meeting of the Ibero-American network of cyber prosecutors (CiberRed), GLACY+
- 6 – 8 February, Yerevan, Armenia – National workshop to discuss cooperation between CSIRT, law enforcement and private sector from the perspective of cybersecurity strategies / Workshop to expand, complete and maintain the online tool on public/private cooperation, EAP 2018
- 7 – 10 February, Pristina, Kosovo*[1] - Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 12 February, Brussels, Belgium – Public Safety Working Group intercessional meeting, European Commission and ICANN, GLACY+
- 13 February, Montenegro – Meeting to support existing public/private initiatives or establish such mechanisms at domestic level, iPROCEEDS
- 13 – 15 February, Baku, Azerbaijan – National workshop to discuss cooperation between CSIRT, law enforcement and private sector from the perspective of cybersecurity strategies / Workshop to expand, complete and maintain the online tool on public/private cooperation, EAP 2018
- 15 – 16 February, Skopje, "the former Yugoslav Republic of Macedonia" – Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (1st part), iPROCEEDS
- 15 – 17 February, 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

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

[1] This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.