Cybercrime Digest

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

1-15 December 2017

Source: Council of Europe

Date: 7 Dec 2017

Foro recomienda países América fortalecer persecución delitos informáticos

"Más de 150 representantes de gobiernos y autoridades de la justicia penal de 34 países y territorios de las Américas, el sector privado y organizaciones internacionales participaron en el Foro Hemisférico de Cooperación Internacional contra el Delito Cibernético, que tuvo lugar en Santo Domingo, República Dominicana, del 5 al 7 de diciembre de 2017. […] La finalidad del Foro era que los países participantes pudieran aprovechar mejor los programas de aumento de la capacidad que ofrecen las organizaciones internacionales, a fin de aumentar la cooperación y la sinergia entre organizaciones e iniciativas internacionales y dar a conocer experiencias con el fortalecimiento de las actividades de aumento de la capacidad de las autoridades en el ámbito de la justicia penal." READ MORE

RELATED ARTICLES

Presidencia de Republica Dominicana, Inicia Primer Foro Hemisférico de Cooperación Internacional contra Delito Cibernético, 5 Dec 2017

Council of Europe, Hemispheric Forum on International Cooperation against Cybercrime, Conference webpage, 5-7 Dec 2017

El Pais (Costa Rica), Foro recomienda países América fortalecer persecución delitos informáticos, 7 Dec 2017

Gobierno Nacional de Paraguay, Paraguay, presente en trascendente Foro Hemisférico de Cooperación contra los Hechos Punibles Cibernéticos, 5 Dec 2017

Saint-Martin News Network, Ministry of Justice participated in the Hemispheric Forum on International Cooperation against Cybercrime, 14 Dec 2017

Source: ENISA

Date: 15 Dec 2017

Supporting the fight against cybercrime: ENISA reports on CSIRTs and law enforcement cooperation

"These reports address the technical, legal and organisational aspects of the cooperation between Computer Security Information Response Teams (CSIRTs) - in particular national/governmental CSIRTs - and law enforcement agencies (LEAs) and provide recommendations to help them cooperate closer in the fight against cybercrime. The data collected for these reports confirms that CSIRTs and LEAs often exchange information during an incident handling/investigations, both formally and informally and that trust is the key success factor in their cooperation." READ MORE

RELATED ARTICLES

ENISA, Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement, 15 Dec 2017

ENISA, Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects, 15 Dec 2017

Source: Philippines News Agency

Date: 12 Dec 2017

Judges, prosecutors from 14 countries discuss about cybercrime training strategies in Cebu, Philippines

"The event was organized by the DOJ-Office of Cybercrime (OOC) in partnership with the Council of Europe and the European Union under Global Action on Cybercrime Extended (GLACY+) Project. "The workshop aims to equip judges, magistrates, and prosecutors with relevant knowledge to fulfill their roles effectively to keep up with the ever increasing challenges posed by the rise of crimes committed by, through, or with the use of computer systems," DOJ Undersecretary Erickson Balmes said. "The event is set to provide an opportunity to discuss judicial training programs and identify international best practices, key principles to design, implement, develop and assess training strategies on cybercrime and electronic evidence," he said. […] Those participating in the event include representatives of judicial authorities, prosecution service, and relevant training academies and judicial institutions from the member-countries of the GLACY+ Project and the Southeast Asian Region." READ MORE

Source: Europol

Date: 4 Dec 2017

Andromeda botnet dismantled in international cyber operation

"On 29 November 2017, the Federal Bureau of Investigation, in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre, the Joint Cybercrime Action Task Force, Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue). This widely distributed malware created a network of infected computers called the Andromeda botnet. […] Jointly, the international partners took action against servers and domains, which were used to spread the Andromeda malware. Overall, 1500 domains of the malicious software were subject to sinkholing. According to Microsoft, during 48 hours of sinkholing, approximately 2 million unique Andromeda victim IP addresses from 223 countries were captured. The involved law enforcement authorities also executed the search and arrest of a suspect in Belarus." READ MORE

Source: Ministry of the Interior of the Republic of Ghana

Date: 8 Dec 2017

Minister for Interior of Ghana calls for strengthening of collaboration in the ECOWAS sub-region to fight cross-border cyber criminality

"The Minister for the Interior, Mr. Ambrose Dery, has called for the strengthening of collaboration amongst ECOWAS Member States to address issues of cross-border criminality. The Minister made the call on Tuesday, December 5, 2017 at the opening ceremony of the 4-day Joint Introductory Judicial Training of Trainers Course on Cyber-crime and Electronic Evidence. According to him, Joint capacity building programmes, intelligence sharing among investigative agencies and judicial cooperation are areas that required commitment among ECOWAS nations to address regional cyber-crime challenges. He further advocated for the enforcement of the provisions of the ECOWAS Directive on cyber-crimes (Directive C/DIR/1/08/11 of 19 august 2011 on Cyber-crime). "I therefore task ECOWAS to take a leading role in operationalizing the Directive especially in the area of cyber-crime prosecutions. We need to do this alongside the Budapest Convention" he said." READ MORE

Source: The Irish News

Date: 5 Dec 2017

Ireland, new laws propose five years in prison for spreading fake news

"Actively promoting 'fake news' using social media sites will be made an offence under proposals to be brought before the Dáil. New laws tabled by Fianna Fáil would also see the use of internet 'bots' to influence political debate punished with five years in jail or fines of up to €10,000. The legislation also contains restrictions on online political advertising and will require the purchasers of ads to display a transparency notice stating their aim and target audience." READ MORE

Source: Bloomberg

Date: 5 Dec 2017

U.K. Banks Aren't Telling Regulators About All Cyber Attacks

"U.K. banks still aren't telling regulators about all the cyber attacks on the financial services industry despite a ten-fold increase in reports to the Financial Conduct Authority over the last four years."Our suspicion is that there's currently a material under-reporting of successful cyber attacks," Megan Butler, the FCA's director of supervision, said in a speech Tuesday, according to a copy of her remarks on the regulator's website. "The number of breaches relayed back to us looks modest when you set it against the number of attacks on the industry." The number of material attacks reported by firms to the FCA has grown to 49 this year from five in 2014, as hacks become one of the biggest threats to the safety of the financial services industry. The type of hacks is also increasingly concerning for regulators and firms with ransomware making up 17 percent of attacks reported to the regulator." READ MORE

Source: The Guardian

Date: 4 Dec 2017

Bitcoin: UK and EU plan crackdown amid crime and tax evasion fears

"The UK and other EU governments are planning a crackdown on bitcoin amid growing concerns that the digital currency is being used for money laundering and tax evasion. The Treasury plans to regulate bitcoin and other cryptocurrencies to bring them in line with anti-money laundering and counter-terrorism financial legislation. Traders will be forced to disclose their identities, ending the anonymity that has made the currency attractive for drug dealing and other illegal activities. Under the EU-wide plan, online platforms where bitcoins are traded will be required to carry out due diligence on customers and report suspicious transactions. The UK government is negotiating amendments to the anti-money-laundering directive to ensure firms' activities are overseen by national authorities." READ MORE

Source: The Sydney Morning Herald

Date: 8 Dec 2017

New sabotage laws for cyber attacks on Australia's critical infrastructure

"Foreign-backed saboteurs who plant sleeper bugs in critical infrastructure such as telecommunications, power and water that could be mobilised to wreak havoc in the event of a war with Australia will face up to 15 years' jail under the new foreign interference laws. The new laws reflect the changing nature of war, in which the first shots of a major conflict are likely to come electronically and target critical infrastructure used by civilians. They will replace outdated sabotage laws that cover only attacks on defence facilities." READ MORE

Source: Bloomberg Technology

Date: 4 Dec 2017

Tech Companies Identify, Remove 40,000 Terrorist Videos, Images

"Big technology companies have added the digital signatures of 40,000 terrorist videos and images to a shared database as they seek to keep extremist content off their platforms. Facebook Inc., Google's YouTube, which is owned by Alphabet Inc., Microsoft Corp., and Twitter Inc. revealed the numbers in a joint blog post Monday. The four big social media companies, which are part of a group called the Global Internet Forum to Counter Terrorism, announced one year ago that they would begin sharing digital fingerprints – known as hashes – of videos they removed from their platforms for terrorism." READ MORE

RELATED ARTICLES

Facebook, Are We Winning the War On Terrorism Online?, 28 Nov 2017

Source: Security Week

Date: 11 Dec 2017

Database of 1.4 Billion Credentials Found on Dark Web

"Researchers have found a database of 1.4 billion clear text credentials in what appears to be the single largest aggregate database yet found on the dark web. These are not from a new breach, but a compilation of 252 previous breaches, including the previous largest combo list, Exploit.in. The database was found by 4iQ on 5 December 2017. Announcing the discovery, the firm's founder and CTO Julio Casal, said, "This is not just a list. It is an aggregated, interactive database that allows for fast (one second response) searches and new breach imports... The database was recently updated with the last set of data inserted on 11/29/2017. The total amount of credentials (usernames/clear text password pairs) is 1,400,553,869."." READ MORE

Source: The Fiji Times Online

Date: 10 Dec 2017

Fiji, Police Commissioner calls to regulate cyber space

"Police Commissioner Brigadier General Sitiveni Qiliho has called for the regulation of cyber space. While making a presentation during a panel discussion titled 'Regulate Cyber Space?' at the 19th Attorney-General's Conference yesterday, he said a lack of relevant laws and powers was making it difficult for police to investigate cyber crime. […] The Police Commissioner said the Cyber Crimes Unit was conducting investigations under the Crimes Act of 2009. "These sections allow us to investigate complaints with computers and its peripherals which are used to commit an offence. "The provision makes specific mention of computers only and is silent on other digital devices such as mobile phones which have the capacity to store data and connect to the world wide web." He added despite limitations with laws and limited resources, the Cyber Crimes Unit had investigated 156 cases since 2008." READ MORE

Source: Aujourd'hui Le Maroc

Date: 5 Dec 2017

Lancement à Rabat de la campagne nationale de lutte contre la cybercriminalité

"La campagne nationale de lutte contre la cybercriminalité a été lancée, lundi à Rabat, dans le but de sensibiliser les enfants, particulièrement âgés moins de 12 ans, aux dangers de la technologie moderne et promouvoir une culture d'usage sécurisé et équilibré du Web." READ MORE

Source: IT Web

Date: 12 Dec 2017

South Africa, revised cyber crimes Bill irons out sticking points

"The Department of Justice and Constitutional Development has moved to address some sticking points that had tarnished the Cybercrimes and Cybersecurity Bill. The Bill aims to give SA a co-ordinated approach to cyber security, as the country currently has no legislation that addresses cyber crimes. There was an outcry over the initial draft Bill, with several critics saying it was too broad and open to abuse, and it threatened the fundamental democratic spirit of the Internet. However, the Department of Justice and Constitutional Development recently published responses to the public comments received on the Bill, which was tabled in Parliament in February 2017. Several further amendments to the Bill are proposed, including revisions to the offences of unlawful access to data, incitement of violence and cyber bullying." READ MORE

Source: Jeune Afrique

Date: 12 Dec 2017

Algérie: l'inquiétante « Baleine bleue », le jeu qui pousse les jeunes au suicide

"Un jeu morbide sur les réseaux sociaux, le "Blue Whale Challenge", aurait causé le suicide de cinq jeunes. Les parents sont désemparés et le gouvernement enquête. Reportage. […] La spirale meurtrière est telle que le ministre de la Justice a ordonné une enquête. […] D'origine russe, le « Blue Whale Challenge » est un jeu morbide en vogue sur les réseaux sociaux qui consiste à répondre à une série de 50 défis, tel que de se scarifier les bras, de se réveiller la nuit pour regarder des vidéos effrayantes ou encore de se livrer à des rituels de suicide. L'ultime défi consiste à mettre fin à ses jours en se jetant du haut d'un immeuble ou en se pendant haut et court. « La justice s'acquitte de sa mission dans la lutte contre la cybercriminalité et l'Organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication a ordonné en coordination avec les parquets compétents l'ouverture d'une enquête », a indiqué le ministre lors d'un entretien accordé à la télévision algérienne." READ MORE

Latest reports

- European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, Twelfth progress report towards an effective and genuine Security Union, 12 Dec 2017
- European Commission, Article 29 Working Party, Letter to the ICANN CEO on the application of privacy laws to the WHOIS directories, 11 Dec 2017
- Google, New government removals and National Security Letter data, 7 Dec 2017
- Australian Strategic Policy Institute, Cyber Maturity in the Asia Pacific Region 2017, 12 Dec 2017
- MalwareBytes, The New Mafia: Gangs and Vigilantes - A guide to cybercrime for CEOs, December 2017
- Trend Micro, Untangling the Patchwork Cyberespionage Group, 11 Dec 2017

Upcoming events

- 18 – 19 December 2017, Colombo, SRI LANKA – Participation in the annual conference for all the 225 District Judges and Magistrates, organised by the Sri Lanka Judges' Institute, GLACY+
- 18 – 20 December 2017, Ankara, Turkey – Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 20 – 21 December 2017, Skopje, "the former Yugoslav Republic of Macedonia", Regional workshop for sharing good practices on reporting mechanisms existent in IPA region (combined with the 4th meeting of the Project Steering Committee), iPROCEEDS

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