Cybercrime Digest

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

15-30 November 2016

Source: Council of Europe

Date: 18 Nov 2016

Octopus Conference key messages

"Some 300 cybercrime experts from 90 countries, 12 international and 40 private sector, civil society organisations and academia met at the Council of Europe in Strasbourg, France, from 16 to 18 November 2016 for the Octopus 2016 Conference on cooperation against cybercrime. The Conference was opened by Thorbjørn Jagland, Secretary General of the Council of Europe, and commenced with a special session on the occasion of the 15th anniversary of the Budapest Convention on Cybercrime. Andorra deposited the instrument of ratification of the Convention during this session to become the 50th Party to this treaty. Key messages resulting from Octopus 2016 have been shared through the Council of Europe website." READ MORE

Source: All Andorra

Date: 21 Nov 2016

Andorra becomes the 50th country as a member State of the Budapest Convention on Cybercrime

"Andorra becomes the 50th country as a member State of the Budapest Convention on Cybercrime. The document was signed in Strasbourg during the international conference, 16-18 November 2016. General principles of international cooperation involve the widest possible cooperation between the parties in criminal cases, the investigation or prosecution of criminal offenses related to computer systems and data, as well as the collection of evidence of criminal offense in electronic form." READ MORE

Source: ComputerWorld

Date: 29 Nov 2016

Upgraded Mirai botnet disrupts Deutsche Telekom by infecting routers

"A new version of Mirai -- a malware that's been enslaving poorly secured IoT devices -- has found a new victim: vulnerable internet routers from Germany's Deutsche Telekom. The spread of the new strain of Mirai has caused internet connection problems for close to a million Deutsche Telekom customers, the company reported on Monday. Deutsche Telekom blamed the disruption on the notorious malware, which has already been found infecting more than 500,000 internet connected devices, including DVRs and surveillance cameras." READ MORE

RELATED ARTICLES

Deutsche Telekom, Information on current problems, 28 November 2016

Boingboing, Two hackers are selling DDoS attacks from 400,000 IoT devices infected with the Mirai worm, 28 November 2016

Source: EUROPOL

Date: 22 Nov 2016

178 Arrests in successful hit by Europol, Eurojust and European Banking Federation against Money Muling

"Supported by Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT), as well as Eurojust and the European Banking Federation (EBF) the second coordinated European Money Mule Action (EMMA) culminated in the arrest of 178 individuals. Law enforcement agencies and judicial authorities from Bulgaria, Croatia, France, Germany, Greece, Hungary, Italy, Latvia, Moldova, the Netherlands, Poland, Portugal, Romania, Spain, United Kingdom, Ukraine, the United States Federal Bureau of Investigation (FBI) and United States Secret Service participated in the international operation. Across Europe, 580 money mules were identified and the national law enforcement agencies interviewed 380 suspects in the course of the action week (14-18 November 2016), with overall reported losses amounting to EUR 23 million. […] The successful hit on this wide-spread crime was supported by 106 banks and private partners." READ MORE

Source: Vanuatu Daily Post

Date: 28 Nov 2016

Vanuatu's Cybercrime Bill "Unsafe"

"The current bill [which is going to be tabled on the next ordinary Parliament session…] makes a general mention of international cooperation in one provision, but does not provide the legislative language necessary for international cooperation or mutual legal assistance. […] Intellectual property and digital copyright, which are of paramount importance to preserve Vanuatu's cultural and artistic heritage, are entirely missing from the text. […] Regulatory powers introduced in the Models give governments and public authorities sweeping, overly broad and intrusive powers to block access to information at their absolute discretion without any safeguards, judicial or other independent supervision, due process provisions, limits to scope or duration and in a disproportionate manner" READ MORE

RELATED ARTICLES

Council of Europe, Report on cybercrime Model Laws, December 2014

Source: News Ghana

Date: 24 Nov 2016

Cabinet approves Ghana's accession to Budapest Convention

"Cabinet has approved Ghana's accession to the Budapest Convention on cyber crime, Mr Felix Ofosu Kwakye, a Deputy Minister of Communication has announced. The Convention pursues as a matter of priority a common criminal policy aimed at protecting countries against cyber crime by adopting appropriate legislation and fostering international cooperation. […] "A national cyber security centre envisaged in the Policy and Strategy will become the central point of coordination and enforcement of standards as we continue to fight against cybercrime," he said. Mr William Tevie, the Director General, National Communication Authority said this year, Ghana received a delegation from the Council of Europe to support Ghana ascend to the Budapest Convention." READ MORE

Source: The Guardian

Date: 29 Nov 2016

UK Internet Surveillance Bill Becomes Law

"The home secretary, Amber Rudd, hailed the Investigatory Powers Act 2016 as "world-leading legislation" that provided "unprecedented transparency and substantial privacy protection". But privacy campaigners claimed that it would provide an international standard to authoritarian regimes around the world to justify their own intrusive surveillance powers. The new surveillance law requires web and phone companies to store everyone's web browsing histories for 12 months and give the police, security services and official agencies unprecedented access to the data." READ MORE

Source: EUROPOL

Date: 17 Nov 2016

International computer fraud, forgery and money laundering ring dismantled

"On 15 November, prosecutors from the Romanian Territorial Office Vâlcea of the Directorate for Investigating Organized Crime and Terrorism (DIICOT), acting within a joint investigation team (JIT) set up with the support of Eurojust, carried out an operation concerning an organised crime group (OCG) specialised in computer fraud, forgery and money laundering. The operation was also supported on-the-spot by Europol. A total of 64 house searches were carried out and 64 suspects were brought to the Public Prosecutors Office in Romania for hearings. Twelve people have been arrested. The OCG was suspected to have been formed in early 2015 and to have defrauded more than 1 000 people of EUR 4.5 million." READ MORE

Source: Politico

Date: 24 Nov 2016

European Commission hacked: what we know and don't know

"The European Commission was the victim of a "large scale" cyberattack, which brought down its internet access for hours Thursday as the institutions braced for more waves. The Commission's IT services sent an email to staff around 6 p.m., which described the attack as a "denial of service … which resulted in the saturation of our internet connection." "No data breach has occurred," a Commission spokesperson told POLITICO. "The attack has so far been successfully stopped with no interruption of service, although connection speeds have been affected for a time." The loss was in man hours. "No one could work this afternoon, since the internet was gone twice, for several hours," one staffer said." READ MORE

Source: African Independent

Date: 28 Nov 2016

Tanzania's social media policing increases the risks of government abuse

"Governments across the region are debating how to respond to new challenges. These include online fraud and the dissemination of hate speech through SMS or social media. Until recently few African countries had legislation related to cybercrime. Police may need further training to deal with digital offences. Citizens will require reliable information about how to stay safe online. In Tanzania the response to these threats has been influenced by political calculations. Expressions of political dissent have been cast as "cybercrime". Thus, for many the most pressing threat to their cyber security may not be fraud or identity theft, but the risk of being arrested for content shared online." READ MORE

Source: The Guardian Nigeria

Date: 18 Nov 2016

Lack of trained manpower hobbles cybercrime law implementation in Nigeria

"Nigerians are yet to feel the impact of the cybercrime law, one year after, no thanks to the dearth of trained judicial and enforcement officers to implement the law. Oluseyi Akindeinde, chief technical officer, Digital Encode, said that the cybercrime law is yet to be properly interpreted by the judges owing to the very technical nature of cybercrimes. "Currently, the judges are being trained in some of the cybercrime related offenses so as to properly adjudicate cases that come before them," he said." READ MORE

Source: Irish Legal News

Date: 15 Nov 2016

Ireland to introduce cybercrime legislation 'as soon as possible'

"Justice Minister Frances Fitzgerald opened the Dublin Info Sec 2016 conference with a promise to introduce new cybercrime legislation "as soon as possible". Ms Fitzgerald told the conference: "Earlier this year I published legislation dealing with attacks against information systems. "The Criminal Justice (Offences Relating to Information Systems) Bill defines criminal offences in the area of cyber attacks on information systems and the information held on them and seeks to establish effective penalties for such offences". The Bill creates new offences relating to unauthorised accessing of information systems, interference with information systems or with data on such systems, interception of transmission of data to or from information systems, and the use of tools to facilitate the commission of these offences." READ MORE

Source: Reuters

Date: 22 Nov 2016

Thailand seeks to tighten cyber security, raising questions about privacy protection

"Thailand's military government, which has cracked down on online dissent since seizing power in 2014, is pushing ahead with cyber security bills that rights groups say could mean more extensive online monitoring, raising concerns over privacy protection. Amendments to Thailand's 2007 Computer Crime Act to be considered by parliament next month have come under fire from critics who say the bill could give state officials sweeping powers to spy on internet users and restrict online speech. Critics say parliament is likely to approve the amendments because lawmakers voted unanimously to pass the bill in its first reading." READ MORE

Source: The Economic Times

Date: 17 Nov 2016

It is government's obligation to strengthen cyber laws, says Supreme Court Judge in India

"The government needs to strengthen laws in view of huge rise in cyber crimes threatening the country, Supreme Court judge Justice Dipak Misra today said. "When the good exists, the evil has to be around. That idea has provoked some to abuse the Internet. Instances of cyber crime are on the rise and that is quite threatening. " The growth of registration of cases under Information Technology (IT) Act along with the offences under other penal laws has become a menace to the society. The rate of offences has grown by 350 per cent from 2011 to 2015," Justice Misra said while addressing the 'International Conference on Cyberlaw, Cybercrime and Cybersecurity'." READ MORE

Source: Daily FT

Date: 30 Nov 2016

Discussion on consolidated law to combat cyber violence against women in Sri Lanka

"Sri Lanka needs to consolidate its existing laws against harassment and computer crimes in order to introduce one single, all-encompassing law to fight cyber bullying and online harassment of women and children, an expert panel declared yesterday. […] It's not that there aren't laws in Sri Lanka against cyber bullying, expert said, pointing to existing provisions on sexual harassment, criminal intimidation, sexual exploitation of children by "whatever" means - which could be interpreted to include online exploitation - but the need of the hour is to harmonise laws pertaining to cyber bullying." READ MORE

Source: Phone World

Date: 16 Nov 2016

How Cybercrime Bill will protect women in Pakistan?

"Cybercrime and the cyber bullying are increasing day-by-day and women are often the main target. It is believed that more than 80% of the victims in Pakistan are female and children. […]Now that the Cybercrime Bill is approved there is a ray of hope that this will protect women on the internet. The bill covers different aspects related to cybercrime. It includes a special endowment for the defense of women. The bill article makes it illegal by law to threaten a woman with sexual ferocity or post images of a woman online without her "definite or implicit consent." READ MORE

RELATED ARTICLES

Geo News, First conviction in Lahore under cybercrime law, 30 November 2016

Latest reports

- GLACY+ Launching movie, 2 December 2016
- Council of Europe, The Budapest Convention on Cybercrime at 15: Achievements and Challenges, 16 Nov 2016
- Council of Europe, Octopus Conference 2016: Key Messages, 18 Nov 2016
- UN General Assembly, The right to privacy in the digital age, adopted on 16 Nov 2016
- Global Commission on Internet Governance, Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study, November 2016
- D. Svantesson, Preliminary Report: Law Enforcement Cross-Border Access to Data, 24 Nov 2016
- Freedom House, Freedom of the Net 2016, November 2016

Upcoming events

- 6-8 December 2016, Strasbourg, France – Meeting of the Cybercrime Working Group of the Pompidou Group, EAP II
- 6-9 December 2016, Zapopan, Mexico – 11th meeting of the Internet Governance Forum, Cybercrime@Octopus
- 8-9 December 2016, Pristina, Kosovo* – Workshop on inter-agency and international cooperation for search, seizure and confiscation of online crime proceeds, iPROCEEDS
- 12-13 December 2016, Bucharest, Romania - Regional workshop on Money Laundering Risks related to New Technologies, iPROCEEDS
- 15-16 December 2016, Skopje, "the former Yugoslav Republic of Macedonia" – Workshop on inter-agency and international cooperation for search, seizure and confiscation of online crime proceeds, 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

*The designation is without prejudice to positions on status, and is in line with the ICJ Opinion on the Kosovo Declaration of Independence.