Cybercrime Digest

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

16-31 December 2016

Source: Council of Europe

Date: 16 Dec 2016

Senegal accedes to the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism

"Senegal deposited the instrument of accession and became the 51st State Party to the Budapest Convention on Cybercrime. Another 16 have either signed or been invited to accede.

Senegal also deposited the instrument of accession to the Protocol on Xenophobia and Racism. 26 States are now Party to the Protocol." READ MORE

Source: DW

Date: 21 Dec 2016

European Court of Justice rules against mass data retention in EU

"The Court of Justice of the European Union ruled on Wednesday that laws allowing for the blanket collection and retention of location and traffic data are in breach of EU law. In their decision, the justices wrote that storing such data, which includes text message senders and recipients and call histories, allows for "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained. Such national legislation exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society," the Luxembourg-based court said. EU member states seeking to fight a "serious crime" are allowed to retain data in a targeted manner but must be subject to prior review by a court or independent body, the EU's top court said. Exceptions can be made in urgent cases." READ MORE

Source: U.S. Department of State

Date: 23 Dec 2016

"Joint Elements" from the EU-U.S. Cyber Dialogue

"On the occasion of the third meeting of the EU-U.S. Cyber Dialogue in Brussels on December 16, the participants jointly affirmed specific areas of cooperation as follows: International Security in Cyberspace […], Cyber Capacity Building […], Internet Governance […], Promotion and Protection of Human Rights Online […], Combatting Cybercrime […], Cyber Resilience […], Transatlantic cyber policy research cooperation. Both the European Union and the United States stressed the importance of protecting cyberspace from abuse and criminal activities for the benefit of our economies and societies, and therefore the need for law enforcement and judicial authorities to have effective tools to investigate and prosecute criminal acts related to cyberspace. Both participants affirmed their commitment to promote the Convention on Cybercrime ("Budapest Convention") in the fight against cybercrime, including by working together in international fora." READ MORE

Source: Le Monde

Date: 27 Dec 2016

L'OSCE victime d'une attaque informatique majeure

"[…] L'Organisation pour la sécurité et la coopération en Europe (OSCE), un outil diplomatique issu de la guerre froide quelque peu oublié, est revenu, depuis 2014, au cœur des enjeux stratégiques internationaux à la faveur du conflit en Ukraine.

L'organisation présente suffisamment d'intérêt pour avoir fait l'objet d'un piratage sophistiqué et de grande ampleur, selon des informations obtenues par Le Monde et confirmées par l'OSCE, mardi 27 décembre. «Il semble que l'organisation s'en soit rendu compte vers la fin du mois d'octobre», explique sa porte-parole, Natacha Rajakovic, qui se garde de donner trop de détails, notamment sur les commanditaires de l'intrusion. En cette période de fêtes, l'OSCE est à moitié vide et la plupart des employés sont rentrés dans leur pays d'origine. Ils peuvent désormais craindre que les pirates aient eu accès à leurs courriers électroniques, leurs dossiers et leurs mots de passe." READ MORE

Source: Interpol

Date: 30 Dec 2016

Interpol operation targeting phone and e-mail scams nets 1,500 arrests

"More than 1,500 people have been arrested in an INTERPOL-coordinated operation targeting multi-million euro telephone and e-mail scams across Asia. Operation First Light 2016 saw police across the region conduct raids of suspicious call centres, with the largest in the Philippines where police arrested some 1,300 Chinese nationals working in a single location as part of a massive criminal operation. The suspects were engaged in a range of criminal activities from the same building, including telephone scams aimed at victims in China, money laundering and illegal online gambling. " READ MORE

Source: Europol

Date: 20 Dec 2016

Darknet arms vendor arrested in Slovenia with support of Europol

"Last week, a 39-year old vendor and his 33-year old accomplice were arrested in Ljubljana by the Slovenian National Police for allegedly selling lethal weapons and explosives on the dark web. A large quantity of weapons uncovered during the house searches were also seized, including automatic and semiautomatic guns, hand grenades and ammunition. The two men, both Slovenian nationals, sold weapons on the Darknet which were then sent via postal mail to buyers in the EU (France, the Netherlands, Sweden and the United Kingdom) and beyond (Norway). The pair also sold ammunition to the weapons they advertised. The transactions were paid for in Bitcoin." READ MORE

Source: International Business Times

Date: 19 Dec 2016

Germany's courts should combat fake news on social media immediately, justice minister says

"Germany's Justice Minister Heiko Maas said local courts must crack down on the spread of fake news through social media platforms immediately. In an interview with the Bild am Sonntag newspaper, published on Sunday (18 December), the Social Democrat in conservative Chancellor Angela Merkel's Christian Democratic Union (CDU) coalition has said that laws against defamation in Germany are much firm than those in the US. "Defamation and malicious gossip are not covered under freedom of speech," Maas said. "Justice authorities must prosecute that, even on the internet. Anyone who tries to manipulate the political discussion with lies needs to be aware [of the consequences.]" […] German intelligence officials have also reported a "striking increase" in Russian propaganda and targeted cyberattacks designed to destabilise German society and influence the federal election in 2017." READ MORE

Source: Finextra

Date: 21 Dec 2016

Italian banks set up cybercrime response team

"The Bank of Italy, together with the Italian Banking Association and the ABI Lab Consortium, signed an agreement in Rome today to strengthen cooperation on cybersecurity. The objective is to ensure greater security for operators in Italy's banking and financial sectors and for the households, businesses and general government departments that use digital services. The agreement - signed by the Senior Deputy Governor of the Bank of Italy, Salvatore Rossi, the Director General of ABI, Giovanni Sabatini, and the President of ABI Lab, Pierfrancesco Gaggi - will see the creation of a highly specialized Computer Emergency Response Team (CERT) for Italy's financial sector, to prevent and combat cyber threats linked to the development of new technologies and to the digital economy." READ MORE

Source: NL Times

Date: 21 Dec 2016

Dutch Parliament approves bill to hack criminal suspects

"A majority in the Tweede Kamer on Tuesday approved a bill that allows the police to hack suspects in a criminal case. A stricter variant of the law was voted in, in which the police are obliged to immediately report software vulnerabilities to its developers, NU.nl reports. The law is called Cybercrime III and states that the police can hack the computers of suspects in criminal investigations. This involves suspects in cybercrime, but also other forms of serious crime that carry a penalty of at least 4 years in prison. In its original form, the law gave the police the power to make use of software vulnerabilities that the developer are unaware of, so-called zero-days, without reporting the problems to the developers." READ MORE

Source: Reuters UK

Date: 16 Dec 2016

Turkey's Akbank faces $4 million hit from attempted cyber heist

"Hackers targeted Turkey's Akbank via the SWIFT global money transfer system in an attack which the bank said had not compromised customer data but would cost it up to $4 million. Banks globally face a growing threat from cyber attacks, more of which have succeeded since February's $81 million heist from the Bangladesh central bank. It was not immediately clear how much, if any, money had been stolen from Akbank, Turkey's third-largest listed bank by assets and it would not give any further details beyond confirming it had been targeted in a SWIFT attack on Dec. 8. Akbank said in a statement on Thursday it had immediately taken preventive measures and informed authorities, that its systems were working properly and there was no loss to customers." READ MORE

RELATED ARTICLES

Hurriyet Daily News, Major cyber-attack on Turkish Energy Ministry claimed, 31 December 2016

Source: Reuters

Date: 20 Dec 2016

Ukraine investigates suspected cyber attack on Kiev power grid

"Ukraine is investigating a suspected cyber attack on Kiev's power grid at the weekend, the latest in a series of strikes on its energy and financial infrastructure, the head of the state-run power distributor said on Tuesday. Vsevolod Kovalchuk, acting

chief director of Ukrenergo, told Reuters that a power distribution station near Kiev unexpectedly switched off early on Sunday, leaving the northern part of the capital without electricity. A Ukrainian security chief said last week that Ukraine needed to beef up its cyber defenses, citing a spate of attacks on government websites that he said originated in Russia." READ MORE

Source: HackRead

Date: 20 Dec 2016

Anonymous Shut Down Thai Sites Against Internet Censorship, Surveillance Law

"The government of Thailand has been under the hammer of internet activist groups since the parliament approved an amendment to the 2007 Computer Protection Law. There is strong resentment among activists because the Single Internet Gateway project will be implemented by the amended law, which was passed on Friday. The Single Internet Gateway project of the military government requires scanning of the entire digital data from overseas via a junta-controlled entry point. The project has received immense criticism from civil society and internet activist groups alike. After the bill was passed into a law, the websites of the National Security Agency and the Ministry of Defense became inaccessible on Tuesday. It is being reported that six government websites, including the two mentioned above, were DDoSed including the public page of the ruling junta party, National Security Guard website and the webpage of the Ministry of Digital Economy." READ MORE

RELATED ARTICLES

HackRead, Thai Police Arrest 9 Suspects Behind Cyber Attacks on Gov't Sites, 26 Dec

Source: IAfrikan Daily Brief

Date: 21 Dec 2016

Kenya's cyber security and protection Bill withdrawn from debate, so it can go for public consultations

"The Senate Committee on Information and Technology has withdrawn the Cyber Security and Protection Bill 2016 [PDF] to allow the public more time to give their views on the proposed law. The committee Chair, Hon. Mutahi Kagwe, pointed out that there are loopholes in the proposed bill and as such, it cannot be passed as the public was not involved in the process. […]. The Computer and Cyber Crimes Bill 2016 proposes wide-ranging offences relating to aspects of unauthorised access or access to the internet in order to commit further offences involving protected computer systems, child pornography, cyber stalking and computer fraud, which aims at protecting Kenyans from cyber bullying. […]The Bill borrows heavily from international standards and global scholars. It has the input of experts from Europe, Inter-Agency Committee for Formulation on Cyber-crime, the Budapest Convention on Cybercrime and the Council of Europe experts." READ MORE

Source: Daily News Egyot

Date: 19 Dec 2016

Political parties demand swift implementation of controversial cybercrime bill in Egypt

"Several political parties and factions have demanded a prompt finalisation and implementation of the cybercrime bill, saying that issuing it has become compelling amid an increase in terrorist attacks, state-owned Al-Ahram reported. The bill intends to curb such attacks by cracking down on social media and online communication." READ MORE

Source: Tunis Daily News

Date: 21 Dec 2016

Prime Minister decides on drafting cybercrime bill for Libya

"The Presidency Council has met once again to work on its final ministerial picks for the GNA, to be submitted to parliament in Tobruk. Since it was meeting in Tripoli which he considers insecure, Ali Gatrani did not join his eight colleagues. Earlier this month, another gathering to mull the new cabinet was held in Tunis so that Gatrani could attend. Little detail has been revealed the decisions made at what the PC says was an ordinary scheduled Monday meeting. The ministerial allocations for the 2017 budget was on the agenda along with the lack of cash for banks to issue, the still falling exchange rate and the Council's continuing row with the Central Bank at its governor Saddek Elkaber." READ MORE

Latest reports

- Dan Lohrman, The Top 17 Security Predictions for 2017, 27 December 2016
- U.S. House Judiciary Committee, House Energy and Commerce Committee, Encryption Working Group Year-End Report, 20 December 2016
- Access Now, Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa, December 2016
- White Ops, The Methbot Operation, 20 December 2016

Upcoming events

- 16 – 17 January 2017, Dakar, Senegal – Advisory mission and workshop on Cybercrime Policies, GLACY+
- 16 – 17 January 2017, Belgrade, Serbia – Workshop on online financial fraud and credit card fraud, 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

www.coe.int/cybercrime