Cybercrime Digest

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

1-15 December 2016

Source: Europe's World

Date: 2 Dec 2016

Evidence in the cloud and the rule of law in cyberspace: avoiding the 'jungle'

"Criminal justice authorities need to be able to secure electronic evidence, including on servers in the cloud, to protect society and individuals against crime online. The powers to obtain such evidence must be subject to data protection and other safeguards. Proposals to move ahead are now available. […] At the Council of Europe in 2014 the parties to the Budapest Convention on Cybercrime – currently comprising 41 European states as well as Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and USA – established a working group to identify 'solutions on criminal justice access to evidence stored in the cloud and in foreign jurisdictions'." READ MORE

Source: Europol

Date: 1 Dec 2016

'Avalanche' network dismantled in international cyber operation

"On 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Lüneburg Police (Germany) in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust and global partners, dismantled an international criminal infrastructure platform known as 'Avalanche'. […] The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform. The global effort to take down this network involved the crucial support of prosecutors and investigators from 30 countries. As a result, 5 individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries." READ MORE

RELATED ARTICLES

Europol, Operation Avalanche infographic and Operation Avalanche (Technical infographic), 1 December 2016

Source: Europol

Date: 12 Dec 2016

Joint international operation targets young users of DDOS cyber-attack tools

"From 5 to 9 December 2016, Europol and law enforcement authorities from EU Countries and the United States carried out a coordinated action targeting users of Distributed Denial of Service (DDoS) cyber-attack tools, leading to 34 arrests and 101 suspects interviewed and cautioned. Europol's European Cybercrime Centre supported the countries in their efforts to identify suspects in the EU and beyond, mainly young adults under the age of 20, by hosting operational meetings, collating intelligence and providing analytical support. […] The tools used are part of the criminal 'DDoS for hire' facilities for which hackers can pay and aim it at targets at their choosing." READ MORE

Source: Reuters

Date: 8 Dec 2016

ThyssenKrupp secrets stolen in cyber attack

"Technical trade secrets were stolen from the steel production and manufacturing plant design divisions of ThyssenKrupp AG in cyber-attacks earlier this year, the German company said on Thursday. ThyssenKrupp, one of the world's largest steel makers, said it had been targeted by attackers located in southeast Asia engaged in what it said were "organized, highly professional hacker activities". In breaches discovered by the company's internal security team in April and traced back to February, hackers stole project data from ThyssenKrupp's plant engineering division and from other areas yet to be determined." READ MORE

Source: El Universal

Date: 4 Dec 2016

AL y el Convenio del Consejo de Europa sobre ciberdelincuencia: acelerar la adhesión

"Los países de Latinoamérica deberían acelerar y completar el proceso de adhesión al Convenio de Budapest sobre la ciberdelincuencia lo antes posible y demonstrar así su compromiso para proteger el Estado de derecho en el ciberespacio." READ MORE

Source: Excelsior

Date: 7 Dec 2016

Piden a México en Convenio de Budapest, ser más que un observador

"El cibercrimen y otro tipo de delitos como la pornografía infantil o la corrupción se han convertido en problemas transnacionales que requieren de la cooperación entre países para combatirlos, de ahí la necesidad de que México se adhiera a acuerdos como el Convenio de Budapest. "Hace nueve años, en 2007, México expresó su interés de cooperar con otros países para luchar contra el cibercrimen, pero desafortunadamente México nunca ha finalizado el procedimiento para adherirse al Convenio de Budapest", explicó el responsable de la división de ciberdelincuencia del Consejo de Europa y secretario del Comité del Convenio de Budapest, Alexander Seger." READ MORE

RELATED ARTICLES

Informador, Denuncia ciudadana, clave para atacar los ciberdelitos, 7 Dec 2016

Source: Kenya Engineer

Date: 5 Dec 2016

ICT Ministry committed to end cyber and computer insecurities in Kenya

"Government is developing the Computer and Cyber-crime bill 2016 in order to end cyber security and child on-line protection. The bill will provide a legislative framework that will seal loopholes used by cyber fraudster to perpetrate offences in the country. The Bill will also witness arrests and prosecution of offenders as well promote sensitization programmes on cyber security among law enforcers, prosecutors and judicial officers to enable them deal with cyber security effectively. […] The bill, which has input of experts from Europe, Inter-Agency Committee for Formulation on Cyber-crime, the Budapest Convention on Cybercrime and the Council of Europe experts will lend heavily from international standards and global scholars. This will aid Kenya meet international best practices and standards." READ MORE

Source: Fin24Tech

Date: 12 Dec 2016

Cybercrimes Bill passed to Parliament in South Africa

"Cabinet has given the green light to a cybercrimes and cybersecurity bill that has sparked criticism over its potential to curb a free internet. The bill creates about 50 new offences for crimes such as hacking, using financial information to commit an offence, unlawful interception of data, computer related forgery, extortion, terrorist activity and distribution of 'harmful' data messages. […] The bill further gives the South African Police Service and the State Security Agency powers to investigate, search, access and seize the likes of computers, databases or networks, provided they have a search warrant." READ MORE

RELATED ARTICLES

Government RSA, Statement on the Cabinet meeting of Wednesday, 7 Dec 2016

Ministry of Justice RSA, Draft Cybercrimes and Cybersecurity Bill

Source: GFCE

Date: 7 Dec 2016

Cybersecurity and the Fight against Cybercrimes in West Africa: current status, challenges and the future

"The growth in the use and development of ICT goes hand in hand with the rise of cyber related crimes and activities in West Africa. This makes for interesting times in the region, as measures need to be put in place to ensure that ICT growth is not stifled [and] cybercrimes are curbed. A number of cyber related Supplementary Acts to support the secure use of ICT services have been adopted within the Economic Community of West African States (ECOWAS) and are currently under implementation by Member States. The ECOWAS, in collaboration with various partners, is working to ensure the secure use of ICT services among its Member States." READ MORE

Source: CNN Tech

Date: 14 Dec 2016

Yahoo says data stolen from 1 billion accounts

"Yahoo disclosed a new security breach on Wednesday that may have affected more than one billion accounts. The breach dates back to 2013 and is thought to be separate from a massive cybersecurity incident announced in September. Yahoo now believes an "unauthorized third party" stole user data from more than one billion accounts in August 2013. That data may have included names, email addresses and passwords, but not financial information." READ MORE

Source: L'Orient Le Jour

Date: 30 Nov 2016

Liban, la lutte contre la cybercriminalité financière mise surtout sur la prévention

"[…] Les chiffres, rappelés par le secrétaire général de la Commission d'enquête spéciale de la Banque Du Liban, sont édifiants : «En 2011, la CSI a reçu un seul cas de cybercrime financier, alors que, cette année, 137 cas ont déjà été signalés pour un montant d'environ 8 millions de dollars.» […] «Je me demande comment il est possible que des cybercrimes soient jugés en l'absence de loi», s'étonne Manuel de Almeida Pereira, du Conseil de l'Europe. Pour lui, le Liban aurait tout intérêt à adhérer à la convention de Budapest sur la cybercriminalité. «Si le Liban s'engage à respecter la convention, nous pourrons les aider à promulguer une loi sur le cybercrime. Cette démarche aiderait le Liban à coopérer judiciairement avec d'autres États, ce qui semble urgent au vu de l'ampleur du cybercrime dans le pays.»" READ MORE

Source: Chatham House

Date: 8 Dec 2016

Cybercrime: Time For the GCC to Join Global Efforts

"The recent malware attack on Saudi Arabia's transport sector and other government agencies shows yet again that cybercrime remains a major threat for the GCC governments and businesses alike. […] Just a few days after the Saudi attack was revealed, an international coordinated operation managed to successfully dismantle a global cyber-criminal network known as "Avalanche". This was the result of 4 years of investigation and cooperation between police in 30 countries and agencies such as FBI, Europol, Eurojust. Despite the obvious benefits of using international cooperation in cybercrime, the Gulf countries remain outside these international efforts, thereby exposing their governments, corporations and citizens to increased vulnerability." READ MORE

Source: Sunday Guardian Live

Date: 11 Dec 2016

India, 'Digital economy needs stricter cyber laws'

"Cyber experts have warned of a possible increase in incidents of cybercrime and the need for stricter laws than those at present, as India takes tentative steps into a world of digital economy in the aftermath of the demonetisation of Rs 500 and Rs 1,000 notes. At present, cyber laws are governed by Information Technology (IT) Act 2000, which was amended in 2008, which is insufficient to deal with the ground realities of 2016, when a large population has migrated to online transactions and increased use of credit and debit cards and e-wallets. In this new era, cyber experts want a new law to govern digital transactions." READ MORE

RELATED ARTICLES

TeleAnalysis, Cybercrimes In India To Rise By 65% By 2017 : Study, 12 Dec 2016

Source: InTabloid

Date: 30 Nov 2016

Survey Claims that Cyber Crimes in China Grew 969% from 2014 To 2016

"Depending too much over technology pays back, according to the final reports of a survey being done, it is being said that cyber crimes grew at a rate of 969% in China in between the year 2014 to 2016. The reason to these cyber attacks is said to be the new technologies implemented in the households that are vulnerable to cyber hacks as they remain connected to the internet all the day. The global average of Cyber hacks is 13 per day and in China itself it was shown 7 a day out of 440 respondents to the survey." READ MORE

Source: CIO Asia

Date: 12 Dec 2016

Philippines launches National Cybersecurity Plan

"The Philippines' Department of Information and Communications Technology launched on 8 December 2016 the National Cybersecurity Plan 2022. The plan aims to secure the ICT environment by building a robust cybersecurity infrastructure. […] Under the plan, DICT will lead the coordination of national protection, prevention, mitigation, and recovery from cyber incidents; dissemination of domestic cyber threat and vulnerability analysis; security of public infostructure; and investigation of cybercrimes under its jurisdiction. The Department of Justice, the Philippine National Police and the National Bureau of Investigation are jointly in charge of the investigation and prosecution of cybercrimes, as well as enforcement of cybersecurity laws." READ MORE

Source: Finextra

Date: 1 Dec 2016

FS-ISAC sets up Asian threat intelligence chapter with the Monetary Authority of Singapore

"The Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Monetary Authority of Singapore announced today that they will collaborate to establish an Asia Pacific Regional Intelligence and Analysis Centre to encourage regional sharing and analysis of cybersecurity information within the financial services sector. This Singapore-based Intelligence Centre is expected to begin operations in the first half of 2017." READ MORE

Source: Reuters

Date: 2 Dec 2016

Russian central bank loses $31 million in cyber attack

"Hackers stole more than 2 billion rubles ($31 million) from correspondent accounts at the Russian central bank, the bank said on Friday, the latest example of an escalation of cyber attacks on financial institutions around the globe. Central bank official Artyom Sychyov discussed the losses at a briefing, saying that the hackers had attempted to steal about 5 billion rubles." READ MORE

Latest reports

- Venice Commission (Council of Europe), Opinion on the draft Law 161 amending and completing Moldovan Legislation on Cybercrime, 9-10 Dec 2016
- GFCE, Global Cyber Expertise Magazine Issue 2, 7 Dec 2016
- ENISA, Opinion Paper on Encryption, 12 Dec 2016
- ICANN, Report on Syntax and Operability Accuracy of WHOIS Data in gTLDs, 12 Dec 2016
- Ali MA, Arief B, Emms M, van Moorsel A., Newcastle Univesity, "Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?" (see also "Six seconds to hack a credit card"), 2 Dec 2016

Upcoming events

- 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