Cybercrime Digest

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

16-31 March 2019

Source: Europol

Date: 18 Mar 2019

Law enforcement agencies across the EU prepare for major cross-border cyber-attacks

"The possibility of a large-scale cyber-attack having serious repercussions in the physical world and crippling an entire sector or society, is no longer unthinkable. To prepare for major cross-border cyber-attacks, an EU Law Enforcement Emergency Response Protocol has been adopted by the Council of the European Union. The Protocol gives a central role to Europol's European Cybercrime Centre (EC3) and is part of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises. It serves as a tool to support the EU law enforcement authorities in providing immediate response to major cross-border cyber-attacks through rapid assessment, the secure and timely sharing of critical information and effective coordination of the international aspects of their investigations. The EU Law Enforcement Emergency Response Protocol determines the procedures, roles and responsibilities of key players both within the EU and beyond; secure communication channels and 24/7 contact points for the exchange of critical information; as well as the overall coordination and de-confliction mechanism." READ MORE

Source: DN (article translated from Norwegian)

Date: 28 Mar 2019

Norwegian Supreme Court accepts trans-border search of data stored "in the cloud"

"Økokrim may resume the search of Tidal. The Supreme Court has decided on Thursday. "Firstly, we are pleased that the Supreme Court came to the same thing as Økokrim believed" says state prosecutor Henrik Horn in Økokrim. On December 17, Økokrim began to search Tidal's offices. But because Tidal's data servers are located abroad, Tidal appealed the court's decision and thought the search broke with international law. The case has, therefore, major consequences for a number of investigations. "It is important for the police to keep the possibility of being able to search themselves in such situations. It clearly gives us better access to evidence both in favor and against the accused" says Horn. Tidal has sent out the following press release on the Supreme Court's decision: "We are disappointed that the fundamental freedom from cross-border intervention is not protected in the Supreme Court's decision. This case was not about Tidal, but about companies' right to protection in the future. Unfortunately, we did not win this. As previously communicated and confirmed by Økokrim, Tidal is not charged or suspected in the case. We will continue to offer our assistance to Økokrim. We are also in the process of sharing further information with Økokrim and we hope we are approaching a conclusion of the case. "The legal issues that technological developments bring to light through the use of coercive measures aimed at "cloud storage" are little clarified, both in Norwegian law and internationally," writes the Supreme Court. It is pointed out that there are somewhat different practices in countries that it is natural to compare with. In Denmark, the Supreme Court has ruled that the police could, in a specific case, gain access to Messenger and Facebook profiles, even though the information relating to the profiles was located on servers abroad. In Sweden, the practice has been stricter. The Supreme Court has also reviewed current reports from the Council of Europe and the EU. The conclusion is that the police in most European countries have the opportunity to seize servers in other countries. The key is that the police must secure their user name and password so that they can obtain the data through a computer in the country where the possible offense has occurred. The Supreme Court, in its summary of the judgment, writes that the search "would not entail any infringement of the exclusive right of other states to use force on their own territory". The decision clarifies the right to search the data material stored "in the cloud", writes the Supreme Court." READ MORE (News in Norwegian)

Source: Ministère de l'Economie Numérique et de la Poste, Côte d'Ivoire

Date: 19 Mar 2019

Côte d'Ivoire, le ministre Isaac Dé « La Convention de Budapest est un formidable instrument de lutte contre la cybercriminalité »

"Le Ministre de l'Economie Numérique et de la Poste, Monsieur Claude Isaac DE, a procédé, ce mardi 12 mars 2019, au Radisson Blu Airport, à l'ouverture officielle de l'Atelier d'information sur la Convention de Budapest sur la cybercriminalité, dans la perspective de sa ratification par la Côte d'Ivoire. A cette occasion, il a exhorté les participants à se pencher sur tous aspects relatifs à la lutte contre la cybercriminalité, afin d'orienter les décisions de l'Etat ivoirien pour commencer sa ratification. Aussi, a-t-il rassuré le Conseil de l'Europe de sa disponibilité et de l'ensemble des parties prenantes à travailler « d'arrache-pied » en vue de l'adhésion de la Côte d'Ivoire à la Convention de Budapest qui, selon lui, est un formidable instrument de lutte contre la cybercriminalité." READ MORE

Source: Agencia Brazil

Date: 20 Mar 2019

Brazil, US ink cooperation deal on security

"The Ministry of Justice and Public Security signed institutional cooperation agreements with the US Federal Bureau of Investigation (FBI) and the Department of Homeland Security to share information on the work of criminal and terrorist groups. The deals were signed by Brazilian Federal Police Director-General Maurício Valeixo during President Bolsonaro's visit to the US, which ended yesterday (Mar. 19). The initiative aims at the joint fight against transnational organized crime, bolstering existing cooperation efforts between the two nations, the ministry reported. […] Also mentioned were the work of criminal organizations in Brazil and the measures to confront them adopted by the state, […] and the importance of Brazil's joining the Budapest Convention." READ MORE

Source: GRTS

Date: 27 Mar 2019

The Gambia commits to join the international network of the fight against cybercrime

The first draft of a modern legislation on cybercrime and electronic evidence was finalized in The Gambia, fully in line with the international standards provided by the Budapest Convention. The draft law is the result of a 3-day workshop supported by the Council of Europe in the framework of the GLACY+ project. Following the Council of Europe's recommendations issued after the first mission to the Gambia (May 2018), a Drafting Committee was established in January 2019, composed by representatives of various national authorities. A strong commitment was demonstrated by all the concerned institutions during the workshop, which was opened and closed by Hon. Minister of Information and Communication Infrastructure of the Republic of the Gambia, Mr. Ebrima SILLAH. READ MORE

Source: European Commission

Copyright law: the European Commission welcomes modernised rules fit for digital age

Date: 26 Mar 2019

"Today, the European Parliament voted in favour of the new Copyright Directive designed to bring tangible benefits to citizens, all creative sectors, the press, researchers, educators, and cultural heritage institutions. Vice-President for the Digital Single Market Andrus Ansip and Commissioner for Digital Economy and Society Mariya Gabriel welcome the outcome in a joint statement: "We welcome the approval of the Directive on copyright in the Digital Single Market by the European Parliament. This Directive protects creativity in the digital age and ensures that the EU citizens benefit from wider access to content and new guarantees to fully protect their freedom of expression online. […] Today's vote ensures the right balance between the interests of all players – users, creators, authors, press – while putting in place proportionate obligations on online platforms." READ MORE

Source: KrebsOnSecurity

Facebook stored hundreds of millions of user passwords in plain text for years

Date: 21 Mar 2019

"Hundreds of millions of Facebook users had their account passwords stored in plain text and searchable by thousands of Facebook employees — in some cases going back to 2012, KrebsOnSecurity has learned. Facebook says an ongoing investigation has so far found no indication that employees have abused access to this data. Facebook is probing a series of security failures in which employees built applications that logged unencrypted password data for Facebook users and stored it in plain text on internal company servers. That's according to a senior Facebook employee who is familiar with the investigation and who spoke on condition of anonymity because they were not authorized to speak to the press. The Facebook source said the investigation so far indicates between 200 million and 600 million Facebook users may have had their account passwords stored in plain text and searchable by more than 20,000 Facebook employees. The source said Facebook is still trying to determine how many passwords were exposed and for how long, but so far the inquiry has uncovered archives with plain text user passwords dating back to 2012." READ MORE

Source: Graphic Online

Ghana, Communications Ministry commits to tackle cyber crime

Date: 19 Mar 2019

"The Ministry of Communications has declared its resolve to deal ruthlessly with cybercrime to ensure a safe digital space for national development. In line with that, it is pursuing measures, such as leveraging international cooperation, to enhance and accelerate the fight against cybercrime with urgency. The Minister of Communications, Mrs Ursula Owusu-Ekuful, said this in Accra yesterday when she opened a national conference and workshop on the technical implementation of the Budapest Convention, the only international treaty on cybercrime. The two-day workshop, jointly organised by the National Cyber Security Centre of Ghana, under the Ministry of Communications, and the Council of Europe, has brought together more than 100 participants drawn from the Judiciary and the private sector, policy makers and legislators. The participants are to be educated on the Budapest Convention and its implementation gaps, benefits and opportunities." READ MORE

Source: BBC News

Date: 19 Mar 2019

Norway, huge aluminium plants hit by 'severe' ransomware attack

“One of the world's biggest aluminium producers has switched to manual operations at some smelting plants following a "severe" ransomware attack. Hydro, which employs more than 35,000 people in 40 countries, says the attack began on Monday night and is ongoing. Some of the company's factories have been forced to halt production though other facilities, including its power plants, are functioning normally. […] Cyber-security expert Kevin Beaumont told the BBC that if the LockerGoga ransomware had been used, it would likely have been deployed to Hydro's systems manually by an attacker. This could have been done by someone who had gained administrator access to those systems.” READ MORE

RELATED ARTICLES

Security Week, Hydro may have lost $40M after cyberattack, 26 Mar 2019

Source: Dhaka Tribune

Date: 28 Mar 2019

Bangladesh, 3,659 cybercrime cases filled over 6 years, only 25 punished

“Over the last six years, some 3,659 cases related to cybercrime have been lodged in Bangladesh. Of them, 1,575 cases went to the Cyber Tribunal that was established on 28 July, 2013. According to the Police’s Crime Data Management Systems, only 522 cases were settled, and criminals were punished in only 25 cases. […] The spreading of malicious lies through false social media accounts, uploading of private photos without consent, publication and dissemination of defamatory allegations, and uploading of obscene images fall under cybercrimes. ID hacking, stealing of credit card information, intimidation via social media, and luring of unsuspecting people into online financial scams—plus other net-based fraud—also fall under the definition.” READ MORE

Source: The Manila Times

Date: 29 Mar 2019

Cybercrime cases soar in the Philippines

“The number of cybercrime cases investigated by the Philippine National Police (PNP) went up by almost 80 percent last year, according to the PNP’s Anti-Cybercrime Group (PNP-ACG). The PNP-ACG investigated 4,103 cybercrime cases in 2018, which is 79.64 percent higher than the 2,284 cases probed in 2017. In 2013, when the ACG was created, there were only 149 cases reported, the agency said. Of the 4,103 cases, 1,041 were online libel, the most prevalent cybercrime in 2018. This was followed by online scams (1,012), photo and video voyeurism (415), identity theft (395) and online theft (364). The remaining 876 cases were of various offenses.” READ MORE

Source: Moscow Times

Date: 18 Mar 2019

Putin signs 'Fake News,' 'Internet Insults' bills into law

“Russian President Vladimir Putin has signed a controversial set of bills that make it a crime to “disrespect” the state and spread fake news online, Russian media reported on Monday. The bills amending existing information laws overwhelmingly passed both chambers of Russian parliament in less than two months. Observers and some lawmakers have criticized the legislation for its vague language and potential to stifle free speech. The legislation will establish punishments for spreading information that “exhibits blatant disrespect for the society, government, official government symbols, constitution or governmental bodies of Russia”.” READ MORE

Source: The New York Times

Date: 29 Mar 2019

In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering

"Campaigning for Ukraine's presidential election had just begun to heat up when the authorities announced they had thwarted a Russian plot to use Facebook to undermine the vote. Unlike the 2016 interference in the United States, which centered on fake Facebook pages created by Russians in faraway St. Petersburg, the operation in Ukraine this year had a clever twist. It tried to circumvent Facebook's new safeguards by paying Ukrainian citizens to give a Russian agent access to their personal pages. In a video confession published by the S.B.U., Ukraine's domestic intelligence service, a man it identified as the Russian agent said that he resided in Kiev, Ukraine's capital, and that his Russian handlers had ordered him "to find people in Ukraine on Facebook who wanted to sell their accounts or temporarily rent them out."" READ MORE

Source: Europol

Date: 26 Mar 2019

Global law enforcement action against vendors and buyers on the dark web

"Law enforcement from Europe, Canada and the United States joined forces early 2019 to target vendors and buyers of illegal goods on dark web marketplaces. During the course of this operation, international law enforcement agencies made 61 arrests and shut down 50 dark web accounts used for illegal activity. Law enforcement executed 65 search warrants, seizing 299,5 kg of drugs, 51 firearms, and over €6,2 million (almost €4 million in cryptocurrency, €2,2 million in cash, and €35 000 in gold). They also conducted 122 interviews. By coordinating efforts and acting simultaneously, a strong signal has been sent to those active in selling and buying drugs, counterfeit goods, firearms, etc. on the dark web. This coordinated hit shows that if you are conducting illegal activities on the dark web, you can and will be tracked down by law enforcement." READ MORE

Latest reports

- UNODC, 5th meeting of the Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, 27-29 Mar 2019
- Europol and Trend Micro, Cyber-Telecom Crime Report 2019, 21 Mar 2019
- Cour de Comptes Européenne, Défis à relever pour une politique de l'UE efficace dans le domaine de la cyber sécurité, Mars 2019
- University of Cambridge, A survey of the European Union's Artificial Intelligence Ecosystem, Mar 2019
- Bloomberg, The Worst Corporate Hacks of All Time, 18 March 2019
- Kaspersky, Threat landscape for industrial automation systems. H2 2018, 27 Mar 2019
- Dark Reading, DDoS Attack Size Drops 85% in Q4 2018, 19 March 2019

Upcoming events

- 1-2 April, Conakry, Guinea – Country visit and Awareness raising workshop on the Budapest Convention, Cybercrime@Octopus
- 2-4 April, Bucharest, Romania – ECTEG online First Responder Course meeting, CyberSouth
- 2-5 April, Santo Domingo, Dominican Republic – Advice on the streamlining of procedures for MLA related to cybercrime and e-evidence and Advisory mission on mainstreaming cybercrime training modules in the curricula of judicial training institutions, GLACY+
- 2-6 April, Skopje, North Macedonia – Training of trainers on delivery of the basic training module on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 3-4 April, The Hague, Netherlands – GFCE Working Group Meetings 2019, GLACY+
- 3-5 April, Manila, Philippines – In-country workshops on data protection and INTERPOL Tools and Services combined with support on how to strength the 24/7 points of contact for cybercrime and electronic evidence, GLACY+
- 4 April, Ankara, Turkey – Workshop on online financial fraud and credit card fraud, iPROCEEDS
- 4-5 April, Cotonou, Benin – Country visit and Awareness raising workshop on the Budapest Convention, Cybercrime@Octopus
- 8-9 April, Strasbourg, France – Civil Society Conference for building capacities of NGOs to raise awareness regarding online child sexual exploitation and abuse (OCSEA), EndOCSEA@Europe
- 8-10 April, Rabat, Morocco – Regional workshop on cyber threats and trends, statistics (police, judiciary, CERT and private sector) and discussion on the outline of the annual report on the state of threats on cybercrime and electronic evidence including legislation and court decisions, CyberSouth
- 8-12 April, Santiago, Chile – Advanced Judicial Training on cybercrime and electronic evidence for judges, magistrates and prosecutors, GLACY+
- 9-11 April, Beirut, Lebanon – CEPOL Workshop on cyber security, CyberSouth
- 9-11 April, Belgrade, Serbia – Case simulation exercise on cybercrime and financial investigations (for Bosnia and Herzegovina, Montenegro and Serbia), iPROCEEDS
- 11-12 April, Praia, Cape Verde – Cybercrime Forum for CPLP countries, GLACY+
- 15-16 April, Ankara, Turkey – Domestic meeting of 24/7 Contact Point with judges and prosecutors, iPROCEEDS
- 15-16 April, Nanterre, France - Study visit of the Moroccan delegation to the Judiciary Police on the Pharos platform for cybercrime reporting, CyberSouth
- 15-16 April, Podgorica, Montenegro – Introductory training courses on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (2nd part), iPROCEEDS
- 15-16 April, Brussels, Belgium – EU Cyber Forum and GLACY+ Steering Committee, 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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime