Cybercrime Digest

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

1-14 February 2019

Source: European Commission

Date: 5 Feb 2019

Security Union: Commission recommends negotiating international rules for obtaining electronic evidence

"With the majority of criminal investigations requiring access to evidence based online and often outside the EU, there is an urgent need to equip police and judicial authorities with quick and efficient tools fit for modern reality. Following up on the European Council Conclusions from October 2018, the Commission is presenting two negotiating mandates, one for negotiations with the United States and one on the Second Additional Protocol to the Council of Europe "Budapest" Convention on Cybercrime. Both mandates, which need to be approved by the Council, include specific safeguards on data protection, privacy and procedural rights of individuals. […] The Commission is submitting the two recommendations for the negotiating mandates to the Council. The recommendations will now be considered by the Council, which must formally adopt a decision to authorise the Commission to open negotiations in line with the negotiating directives set out in the mandates." READ MORE

RELATED ARTICLES

European Commission, E-evidence - cross-border access to electronic evidence, International negotiations, 5 Feb 2019

Source: Council of Europe

Date: 11 Feb 2019

LE officers from South-eastern Europe, Romania and Turkey trained on Network Investigations

"In the framework of the Joint Project of the European Union and the Council of Europe - iPROCEEDS, in cooperation with the Romania Police Academy, 16 LE officers from the South-eastern Europe, Romania and Turkey, got practical training sessions on network investigations in criminal investigations and enhanced their skills for dealing with cases requiring this particular expertise in international cooperation." READ MORE

Source: Dark Reading

Date: 5 Feb 2019

Over 59K Data Breaches Reported in EU Under GDPR

"The General Data Protection Regulation (GDPR) officially went into effect across the European Union on May 25, 2018. Since then, more than 59,000 personal breaches have been reported to regulators. […] Breaches likely to cause harm to individuals affected must be reported. Failure to comply can cost fines up to €10 million or up to 2% of the firm's global annual turnover for the previous financial year – whichever is higher. In the eight months since GDPR has been applied, 91 reported fines have been imposed. Not all were for personal data breaches. The highest to date was a €50 million fine imposed on Google related to processing personal data for advertising without valid authorization. A German company was fined €20,000 for failing to hash employee passwords, which led to a security breach. The Netherlands reported the most data breaches (15,400 incidents), followed by Germany and the United Kingdom (10,600). Those with the lowest number of breaches reported include Lichtenstein (15), Iceland (25), and Cyprus (35). Cyberattacks reported under GDPR range from minor security breaches to major, publicized hacks affecting millions of individuals." READ MORE

Source: The Register

Date: 4 Feb 2019

European Commission orders mass recall of leaky child-tracking smartwatch

"The European Commission has ordered the recall of a smartwatch aimed at kids that allows miscreants to pinpoint the wearer's location, posing a potentially "serious risk". […] "The mobile application accompanying the watch has unencrypted communications with its backend server and the server enables unauthenticated access to data," the directive said. As a result, data on location history, phone numbers and device serial number can be found and changed. "A malicious user can send commands to any watch making it call another number of his choosing, can communicate with the child wearing the device or locate the child through GPS," the alert warned. It ordered public authorities to "recall the product from end users"." READ MORE

Source: The New York Times

Date: 31 Jan 2019

Russia's Playbook for Social Media Disinformation Has Gone Global

"Russia created a playbook for spreading disinformation on social media. Now the rest of the world is following it. Twitter said on Thursday that countries including Bangladesh and Venezuela had been using social media to disseminate government talking points, while Facebook detailed a broad Iranian disinformation campaign that touched on everything from the conflict in Syria to conspiracy theories about the Sept. 11 attacks. The campaigns tied to various governments — as well as privately held accounts in the United States — followed a pattern similar to Russian disinformation efforts before and after the 2016 presidential election. Millions of people were targeted by content designed to widen political and social divisions among Americans. The global spread of social media disinformation comes in a year when major elections are set to take place in countries including India and Ukraine." READ MORE

RELATED ARTICLES

Politico, Europe hopes to fend off election hackers with 'cyber sanctions', 11 Feb 2019

Bloomberg, Proyecto de Formación del Ejército de trolls para enfrentar guerra mediática en Venezuela, October 2018

Khaosod English, How Fake News and Disinfo Will Affect Thailand's Election, 7 Feb 2019

Source: Reuters

Date: 13 Feb 2019

Cyber attack on Malta bank tried to transfer cash abroad

"Bank of Valletta which accounts for almost half of Malta's banking transactions, had to shut down all of its operations on Wednesday after hackers broke into its systems and shifted funds overseas. Prime Minister Joseph Muscat told parliament the cyber attack involved the creation of false international payments totaling 13 million euros ($14.7 million) to banks in Britain, the United States, the Czech Republic and Hong Kong. […] To minimize risk and review its systems, the Bank of Valletta suspended operations, shuttering its branches on the Mediterranean island, closing ATMs and disabling its website. Muscat said the fact such an important financial institute had gone off line had impacted the economy and caused problems abroad for credit card holders who needed to make payments, such as to hotels." READ MORE

Source: Rumbogt

Date: 5 Feb 2019

Guatemala, Congreso trabaja en una polémica ley contra delitos cibernéticos

“El diputado guatemalteco José Rodrigo Valladares se reunió este lunes con el viceministro de Tecnologías de la Información, Gabriel Juárez, para discutir una Ley Contra la Ciberdelincuencia que ha sido señalada por la “criminalización de periodistas”. El diputado aseguró a Acan-Efe que esta iniciativa será “diferente” a la que inicialmente fue presentada al pleno legislativo el 9 de marzo de 2017, pues aquella careció de un dictamen en la Comisión Ordinaria de Gobernación del Parlamento. La Ley Contra la Ciberdelincuencia “es necesaria”, dijo el diputado, para que Guatemala se adhiera al Convenio de Budapest, que estipula delitos informáticos de la Internet y al que el solicitó integrarse en 2016. La iniciativa fue criticada en 2017 por su “espíritu criminalizador” por diversos entes de prensa y derechos humanos, pues entre tantos otros el artículo 18 establece el delito de “acoso por medios cibernéticos”.” READ MORE

Source: ZD Net

Date: 11 Feb 2019

Russia to disconnect from the internet as part of a planned test

“Russian authorities and major internet providers are planning to disconnect the country from the internet as part of a planned experiment, Russian news agency RosBiznesKonsalting (RBK) reported last week. The reason for the experiment is to gather insight and provide feedback and modifications to a proposed law introduced in the Russian Parliament in December 2018. A first draft of the law mandated that Russian internet providers should ensure the independence of the Russian internet space (Runet) in the case of foreign aggression to disconnect the country from the rest of the internet. In addition, Russian telecom firms would also have to install "technical means" to re-route all Russian internet traffic to exchange points approved or managed by Roskomnazor, Russia's telecom watchdog. Roskomnazor will inspect the traffic to block prohibited content and make sure traffic between Russian users stays inside the country, and is not re-routed uselessly through servers abroad, where it could be intercepted.” READ MORE

Source: HackRead

Date: 2 Feb 2019

World’s largest data dump surfaces on web with 2.2 billion accounts

“It hasn’t even been 15 days since details of the world’s biggest online private data dump were discovered by security researchers and now its second “installment” has posted online. As per the report from Heise.de, a German-language website, the first collection, which was published on January 17 and dubbed as Collections #1 had approx. 770 million or 772,904,991 unique email IDs of people. It also had 22 million usernames and passwords spread across 2,692,818,238 spreadsheet rows contained in 12,000 files. The second collection of data is named Collections #2-5 and has been posted on Interweb. It contains 2.2 billion usernames and passwords and includes roughly 845GB of stolen data.” READ MORE

RELATED ARTICLES

The Register, 620 million accounts stolen from 16 hacked websites now for sale on dark web, 11 Feb 2019

Source: Recorded Future

Date: 8 Feb 2019

China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems

"[…] The regulations, likely evolved to clarify portions of China's 2017 Cybersecurity Law, give the Ministry of Public Security (MPS) broad powers over the computer networks of companies in China. These ostensibly include the authority to remotely conduct penetration testing on almost any business operating in China and copy any information related to user data or security measures found during the inspection. These new provisions specify no limits on the scope of vulnerability or security inspections and require extremely minimal reporting to be provided back to the corporation. Further, the regulations continue to use vague terminology and do not limit the scope of in-person or remote inspections for network security testing. We assess that the combination of existing MSS regulations with these new Cybersecurity Law provisions for the MPS will support Chinese government attempts to both censor and surveil foreign companies." READ MORE

Source: Benin Web TV

Date: 1 Feb 2019

Bénin: un réseau de faux magiciens démantelé par la Police Républicaine

"La Police Républicaine qui s'est mise aux trousses des faux magiciens qui publient à longueur de journée sur les réseaux sociaux des annonces de vente de portefeuilles magiques. L'Office central de répression de cybercriminalité (Ocrc) qui se charge exclusivement de ces genres de situations a démantelé un réseau de cybercriminels béninois qui publient sur les réseaux sociaux des portefeuilles auxquels ils attribuent une puissance magique." READ MORE

Source: Rough Media Labs

Date: 5 Feb 2019

Ghost Squad hackers release +1GB data related to ISIS members, recruiters and sympathizers Online

"Earlier this morning, February 12th 2019, S1ege of Ghost Squad Hackers released a treasure trove of leaked documents compiled as the result of something known as Operation Decrypt ISIS, an exclusive operation unique to Ghost Squad Hackers. In a personal interview with Rogue Media Labs, S1ege explains how the data provided below comes as the result of months of work, time spent quietly working behind the scenes infiltrating ISIS networks, socially engineering its members and compromising their administrators online." READ MORE

Source: Zambia Reports

Date: 3 Feb 2019

Cyber Crack Squad Formed in Zambia

"In order to specifically deal with the growing trend in cyberspace crimes, a special branch called the Special Joint Cybercrime Crack Squad (SJCCS) has been formed by the government of Zambia. […]The Minister has indicated that the SJCCS is an effort of collaboration amongst security agencies and other stakeholder groups. […] The Crack Squad will support the identification of investigative overlaps and eliminate duplicity of resources whilst effecting new investigative approaches to bring about rapid resolution of cybercrime cases and fast-track prosecution of the offenders. This team will help ensure that public digital platforms including social media are not used as vehicles for illegal and harmful activities." READ MORE

Source: Reuters

Date: 1 Feb 2019

Facebook takes down hundreds of Indonesian accounts linked to fake news syndicate

"Facebook Inc has removed hundreds of Indonesian accounts, pages and groups from its social network after discovering they were linked to an online group accused of spreading hate speech and fake news. Indonesian police uncovered the existence of the group, called Saracen, in 2016 and arrested three of its members on suspicion of being part of a syndicate being paid to spread incendiary material online through social media. […] The world's largest social network has been under pressure from regulators around the globe to fight spread of misinformation on its platform. In January, it announced two new regional operations centers focused on monitoring election-related content in its Dublin and Singapore offices. Indonesia is currently in the run-up to a presidential election set to take place in April, with internet watchdogs flagging the impact of fake news as a concern. Indonesia is estimated to be Facebook's third largest markets, with over a 100 million users." READ MORE

Latest reports

- Council of Europe and Romanian Presidency of the Council of European Union, Criminal Justice in Cyberspace, 25-27 Feb 2019
- Council of Europe, Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings, adopted on 30 January 2019
- European Court of Human Rights, Key Cases 2018, February 2019
- European Parliament, LIBE Committee, LIBE Committee Analysis: Challenges of cross-border access to data, 13 Feb 2019
- OECD, Public consultation on draft OECD Recommendation on Digital Security of Critical Activities, Comments accepted through 28 February 2019
- Twitter, Retrospective Review - Twitter, Inc. and the 2018 Midterm Elections in the United States, 31 Jan 2019
- MIT Technology Review, How quantum terrorists could bring down the future internet, 8 Feb 2019
- ABC News, Meet the scammers: Could this be your online lover?, 11 Feb 2019

Upcoming events

- 15 February, Bucharest, Romania – Awareness raising meeting on the Budapest Convention, benefits and challenges for Embassies of priority countries in Romania, CyberSouth
- 18-22 February, Rabat, Morocco – Working group on integration of the judicial training on cybercrime in the national curricula, CyberSouth
- 18-22 February, Bucharest, Romania - ECTEG Regional Training of Trainers: Live Data Forensics, CyberSouth
- 19-22 February, Pristina, Kosovo* - Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 24-28 February, Cairo, Egypt – Participation in the UNODC meeting "Drafting a legislation on the admissibility of digital evidence before terrorism courts", CyberSouth
- 26-27 February, Bucharest, Romania – Criminal Justice in Cyberspace Conference under Romanian Presidency of the Council of the European Union in cooperation with the Council of Europe, Cybercrime@Octopus / GLACY+ / iPROCEEDS / CyberSouth
- 25 February – 1 March, Bogotá, Colombia – INTERPOL Instructor Development Course for Spanish and Portuguese speaking countries, GLACY+
- 28 February, Rome, Italy – Lecture on the Budapest Convention within the Cybersecurity Master program, LUISS, 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

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE