Cybercrime Digest

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

1 - 15 January 2021

Source: Council of Europe

Date: 1 Jan 2021

The Council of Europe's new global Octopus Project has begun!

"The new global Octopus Project on cybercrime and e-evidence has formally commenced on 1 January 2021. Building on the successful implementation of the previous global Cybercrime@Octopus project aimed at assisting countries worldwide to implement the Budapest Convention on Cybercrime and strengthen data protection and rule of law safeguards, the new Octopus Project will also take into account the additional challenges that came to the forefront in the course of 2020. Assistance to the criminal justice authorities from the countries willing to implement the Budapest Convention, its First Protocol on Xenophobia and Racism, its future Second Protocol on enhanced international cooperation and access to evidence in the cloud, as well as related standards; support to the Cybercrime Convention Committee (T-CY); organisation of the Octopus conferences on cooperation against cybercrime; and the development of online tools for the delivery of capacity building activities on cybercrime and electronic evidence are the four main expected outputs of the new Octopus Project." READ MORE

Source: Europol

Date: 12 Jan 2021

Darkmarket: world's largest illegal dark web marketplace taken down

"DarkMarket, the world's largest illegal marketplace on the dark web, has been taken offline in an international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom (the National Crime Agency), and the USA (DEA, FBI, and IRS). Europol supported the takedown with specialist operational analysis and coordinated the cross-border collaborative effort of the countries involved. […] The Central Criminal Investigation Department in the German city of Oldenburg arrested an Australian citizen who is the alleged operator of DarkMarket near the German-Danish border over the weekend. The investigation, which was led by the cybercrime unit of the Koblenz Public Prosecutor's Office, allowed officers to locate and close the marketplace, switch off the servers and seize the criminal infrastructure – more than 20 servers in Moldova and Ukraine supported by the German Federal Criminal Police office (BKA). The stored data will give investigators new leads to further investigate moderators, sellers, and buyers." READ MORE

Source: Bleeping Computer

Date: 12 Jan 2021

Hackers leak stolen Pfizer COVID-19 vaccine data online

"The European Medicines Agency (EMA) today revealed that some of the Pfizer/BioNTech COVID-19 vaccine data stolen from its servers in December was leaked online. EMA is a decentralized agency responsible for reviewing and approving COVID-19 vaccines, as well as for evaluating, monitoring, and supervising any new medicines introduced to the EU. "The ongoing investigation of the cyberattack on EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines belonging to third parties have been leaked on the internet," EMA said today." READ MORE

Source: Council of Europe

Date: 8 Jan 2021

African Network of DPAs focus on the use of personal data in political campaigning and elections

"Consumer and electoral voter data are increasingly being used for 'data driven' decision making to strategically target people in the process of political campaigning. As more and more people connect online and access digital services, the variety, volume and intimacy of data generated and captured about individuals may be used to influence them for political purposes. Data and access to individuals that digital connectivity brings, is a powerful mix in political campaigning enabling the profiling and (micro) targeting of individuals. But how effective are these new forms of political campaigning and what are the concerns they raise? On 7 January 2021, a workshop organised with the African Network Data Protection Authorities has explored key issues, challenges and considerations in the use of personal data in political campaigns, including voter surveillance, drawing from experiences in Africa and beyond and 100 participants discussed lessons that can be learnt to support data protection authorities across Africa. This workshop was the 3rd of monthly on line workshops on a selection of themes of particular relevance to the African region, on the basis of the principles set forth by Convention 108+, organised in co-operation with the African Network Data Protection Authorities and the support of the Glacy+ Global Action on Cybercrime Extended Programme" READ MORE

Source: The Verge

Date: 12 Jan 2021

FBI received over 100,000 pieces of digital evidence after Capitol attack

"The Justice Department has received over 100,000 pieces of digital evidence following last week's deadly attack on the US Capitol. Shortly after a pro-Trump mob stormed the Capitol last Wednesday, the FBI posted a tweet requesting any information that could help identify people who participated in the riot. As of Tuesday, the FBI said it received more than 100,000 pieces of digital evidence in the wake of that request. […] In the days following the Capitol attack, tech companies and social media platforms have removed thousands of conspiratorial accounts and individuals. Over the weekend, Apple and Google removed the right's favored social media app, Parler, from their app stores. Shortly after, Parler's domain registrars pulled the plug on the site as well, forcing it offline until it found new hosting on Monday. Twitter banned over 70,000 accounts for pushing QAnon-fueled conspiracies on its platform." READ MORE

RELATED ARTICLES

Harvard Business Review, Are We Entering a New Era of Social Media Regulation?, 14 Jan 2021

Source: DW

Date: 12 Jan 2021

Uganda bans social media ahead of election

"Uganda's communications regulator ordered the country's internet service providers to block all social media platforms until further notice, according to a letter seen by news agencies AFP and Reuters. The letter told telecommunications firms to "immediately suspend any access and use" of the apps and sites. Both Reuters and AFP cited sources saying the government made it clear that the ban was in retaliation for Facebook's decision to delete some government-linked accounts. Facebook said it removed them for seeking to manipulate public debate ahead of the election, adding that they were tied to the Ministry for Information and Technology." READ MORE

Source: Council of Europe

Date: 15 Jan 2021

Series of Workshops on Crime Proceeds Online finalized in the Eastern Partnership Region

"As the Eastern Partnership region becomes increasingly integrated into the global economy and with increasing number of people from these countries with daily access to cyberspace, financial crime with the use of information technology, computer systems and data is becoming increasingly prevalent. Effectiveness of fighting such forms of cybercrime depends on many factors, including timely reporting and follow-up of such criminal activity, strong action aimed at seizing proceeds of crime and fighting money laundering, as well as formal and informal cooperation between public institutions and between the public and private sector. With the Workshop on online fraud, crime proceeds and reporting mechanisms for Azerbaijani authorities on 14-15 January 2021, the CyberEast project has closed the series of similar workshops in the Eastern Partnership region, which started in March 2020. " READ MORE

Source: Agence Europe

Date: 11 Jan 2021

Portuguese Presidency of EU Council prepares for negotiations on the e-evidence Regulation

"The Portuguese Presidency of the Council of the EU has started preparing its strategy for interinstitutional negotiations - due to start soon - with the European Parliament on the Commission's proposal for a Regulation to facilitate access to electronic evidence in criminal investigations." READ MORE

Source: Computer Weekly

Date: 8 Jan 2021

UK, Government use of 'general warrants' to authorise computer and phone hacking is unlawful

"The security and intelligence services cannot use "general warrants" to indiscriminately hack into large numbers of mobile phones and computers in the UK, judges have decided. The High Court ruled on 8 January that it was unlawful for GCHQ and MI5 to use the warrants issued under Section 5 of the Intelligence Services Act (ISA) to interfere with electronic equipment and other property. The decision, described by Privacy International as a major victory for the rule of law, follows a five-year legal battle by the non-governmental organisation (NGO) to challenge the legality of warrants that can be used to hack a broad classes of computers and mobile phones. The judgment means that targets for equipment interference – government language for hacking – will have to be scrutinised by a secretary of state, rather than being left to the discretion of intelligence agencies." READ MORE

Source: U.S. Department of Justice

Date: 7 Jan 2021

Russian hacker sentenced to 12 years in prison for involvement in massive network intrusions

"Audrey Strauss, the Acting United States Attorney for the Southern District of New York, announced today that ANDREI TYURIN, a/k/a "Andrei Tiurin," was sentenced in Manhattan federal court to 144 months in prison for computer intrusion, wire fraud, bank fraud, and illegal online gambling offenses in connection with his involvement in a massive computer hacking campaign targeting U.S. financial institutions, brokerage firms, financial news publishers, and other American companies. […] From his home in Moscow, Tyurin played a major role in orchestrating and facilitating an international hacking campaign that included one of the largest thefts of U.S. customer data from a single financial institution in history, stealing the personal information of more than 80 million J.P. Morgan Chase customers." READ MORE

Source: Council of Europe

Date: 16 Dec 2020

Kiribati focuses on aligning cybercrime legislation with international standards

"With the aim to align this bill with the international standards provided by the Budapest Convention, Kiribati requested technical support to the Council of Europe and to the Australian Attorney General's Department, who teamed up in the framework of the GLACY+ Project, to review the current draft and to produce a set of relevant recommendations. The results of such study were presented and discussed with the representatives from the criminal justice sector and the legislators of Kiribati, during a three days' workshop, organized online on 9, 10 and 16 December." READ MORE

Source: Dhaka Tribune

Date: 5 Jan 2021

Cybercrime in Bangladesh: Most accused go unpunished

"Lack of required skill and efficiency of investigating officers and prosecution blamed. Although Bangladesh is witnessing a rising trend of cybercrimes, most of the accused are being discharged or getting acquittal in the cases related to the crimes thanks to the inept role of the prosecution and the police. Legal experts said settlement outside the court, lack of skill of prosecution lawyers, and inability of the law enforcers in handling such cases, pave the way for the criminals to evade punishment. According to Cyber Tribunal (Bangladesh) in Dhaka, a total of 259 cases were disposed of in the last eight years since its inception in 2013. Among those, the accused were discharged in 124 cases and acquitted in 114 lawsuits as the prosecution failed to prove the charges against them." READ MORE

Source: gob.pe

Date: 1 Jan 2021

Peru: Ministerio Público dispuso la creación de una Unidad Fiscal Especializada en Ciberdelincuencia

"La Unidad empezará a funcionar a partir del 15 de febrero y dependerá administrativa y funcionalmente de la Fiscalía de la Nación y brindará un tratamiento especializado y un acompañamiento técnico a los fiscales en la indagación de los delitos informáticos –que se han incrementado en los últimos tiempos, especialmente durante la pandemia del COVID-19– y en casos en los que la obtención de prueba digital sea determinante para la investigación." READ MORE

RELATED ARTICLES

El Peruano Fortalecen investigación fiscal ante casos de ciberdelincuencia, 2 Jan 2021

Source: BBC.com

Date: 15 Jan 2021

Operation Spalax: Targeted malware attacks in Colombia

"In 2020 ESET saw several attacks targeting Colombian entities exclusively. These attacks are still ongoing at the time of writing and are focused on both government institutions and private companies. For the latter, the most targeted sectors are energy and metallurgical. The attackers rely on the use of remote access trojans, most likely to spy on their victims. They have a large network infrastructure for command and control: ESET observed at least 24 different IP addresses in use in the second half of 2020. These are probably compromised devices that act as proxies for their C&C servers." READ MORE

Source: Bitdefender

Date: 12 Jan 2021

Over 200 Million Facebook, Instagram and LinkedIn Profiles Exposed

"Chinese social media management company Socialarks leaked personally identifiable information of over 200 million Facebook, Instagram and LinkedIn users, according to researchers from SafetyDetectives. The data leaked through an unsecured ElasticSearch harbored 408GB of personal data of regular users, social media influencers and even celebrities. Investigators found that the leaked data appeared to have been scraped from popular social media platforms, in violation of the terms of service of the social media giants. The leaky database included the following information: 81,551,567 Facebook account profiles; 66,117,839 LinkedIn user profiles; 11,651,162 Instagram aficionados accounts." READ MORE

Source: DevOps

Date: 12 Jan 2021

The growing role of AI and ML in cybersecurity

"As cyber threats are evolving more every day, it has now become necessary to look at Artificial Intelligence (AI) and Machine Learning (ML) to protect systems and give organizations the best security possible. AI is slowly growing and is starting to be used in many sectors, such as the medical industry or the car industry. It is time that AI helps fight against cyber-attacks. With the advancements of technology and the lockdown, cybersecurity needs to be the top priority for businesses. Now, more than ever, organizations from technology companies to social media websites, have started to use AI in order to stop cyber-attacks. By implementing AI within security systems, businesses can learn from the data collected and use it to their advantage. AI, alongside ML and security platforms, can become a really powerful tool to prevent hackers and cybercriminals from stealing private data and information." READ MORE

Latest reports

- European Medicines Agency, Cyberattack on EMA - update 5, 15 Jan 2021
- United States National Security Agency (NSA), 2020 Cybersecurity Year in Review, 11 January 2021
- Cybersecurity and Infrastructure Security Agency (CISA), Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services | CISA, 14 January 2021
- Government Technology, Top 21 Security Predictions for 2021, 22 December 2020
- Intezer, A Rare Look Inside a Cryptojacking Campaign and its Profit, 13 Jan 2021
- CircleID, Internet Governance Outlook 2021: Digital Cacophony in a Splintering Cyberspace, 08 January 2021

Upcoming events

- 18-20 January, C-PROC/Ukraine, (on-line), Training on international cooperation on cybercrime and electronic evidence for investigators, prosecutors and judiciary, CyberEast
- 19 January, C-PROC/Turkey (on-line), Meeting on the assessment of the collection and investigation/ handling of electronic evidence, iPROCEEDS-2
- 20 January, C-PROC/ITALY, (on-line), Lecture at the University of Naples on "Cybercrime and e-evidence: the criminal justice response", GLACY+

- 25-27 January, C-PROC/Georgia, (on-line), Training on international cooperation on cybercrime and electronic evidence for investigators, prosecutors and judiciary, CyberEast
- 26 January, C-PROC/ North Macedonia, (on-line), Meeting on the assessment of the collection and investigation/ handling of electronic evidence, iPROCEEDS-2
- 27-29 January 2021, C-PROC/ Serbia, (on-line), Business analysis CERT/LEA, iPROCEEDS-2
- 27-29 January 2021, C-PROC/ Serbia, (on-line), Guidelines and procedures on sharing of data by CERTs/CSIRTs with criminal justice authorities, iPROCEEDS-2
- 28 January, C-PROC, (on-line), GLACY+ Steering Committee, GLACY+
- 28 January, C-PROC/Ukraine, (on-line), Workshop with Ukrainian authorities on cybercrime /cybersecurity strategy and action plan (with CyberSecurity EAST), CyberEast
- 28-29 January, C-PROC/Azerbaijan, (on-line), Workshop with personal data protection authorities and national communications regulators on trust and cooperation, CyberEast
- 29 January, C-PROC/Moldova, (on-line), Workshop with Moldovan authorities on the reform of criminal procedure legislation, CyberEast
- 29 January, C-PROC, (on-line), Series of 8 thematic monthly workshops for the International Network of the National Judicial Trainers (1/8), GLACY+
- By 31 January (date TBC), C-PROC/INTERPOL, (on-line), Series of Webinars on Encryption (FR), GLACY+
- By 31 January, T-CY: Support of the T-CY work on negotiation of a 2nd Additional Protocol to the Budapest Convention, T-CY, Octopus Project
- By 31 January, C-PROC: Finalization of the proof of concept of the online training platform on cybercrime, Octopus Project
- By 31 January, C-PROC, Initiation of the work on country profiles on online child sexual exploitation and abuse, Octopus Project, EndOCSEA@Europe

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of January have been rescheduled to a later date.

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