Cybercrime Digest

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

16 – 28 February 2021

Source: Scoop

Date:18 Feb 2021

New Zealand to Join the Council of Europe Convention on Cybercrime

"Cybercrime is increasing every year. International cooperation on tackling cybercrime is essential because criminals frequently operate across borders," Justice Minister Kris Faafoi says.[…] The decision progresses a recommendation by the Royal Commission of Inquiry into the Christchurch terror attack to accede to the Convention.[…] By creating a common framework for tackling computer crimes, and with common powers for obtaining electronic evidence, the Convention strengthens international cooperation on a wide range of criminal investigations, underpinned by international and domestic human rights laws." READ MORE

RELATED ARTICLES

Department of the Prime Minister and Cabinet of New Zealand, Cabinet Decision CBC-20-SUB-0129, 18 Feb 2021

Source: Euractiv

Date: 22 Feb 2021

Increased online criminality makes e-Evidence rules urgent: EU terrorism chief

"Negotiators from the European Council and the European Parliament are currently attempting to hammer out an agreement on the so-called 'e-Evidence' regulation, which will allow authorities based in one EU nation to issue order requests to service providers based in other member states, for access to electronic data to be used in criminal prosecutions. […] Technology, during the pandemic, is more than ever a significant means for terrorists to recruit, spread extremist propaganda, communicate and share instructions for attacks or raise funds" READ MORE

Source: Council of Europe

Date: 25 Feb 2021

Crypto speaks French: rolling out the new edition of INTERPOL GLACY+ Technical Webinars

"INTERPOL has resumed the series of technical webinars on cryptography delivered under the GLACY+ project to Criminal Justice Authorities, this time targeting French speaking professionals from more than 30 countries.[…] The webinars were designed so as to respond to real professional needs noticed in the last years, since cryptography is a subject less covered during professional trainings". READ MORE

Source: Council of Europe

Date: 25 Feb 2021

CyberSouth: Regional Workshop on interagency cooperation on the search, seizure and confiscation of on-line crime proceeds

"The goal of this meeting was to familiarize the project countries with international standards on seizing cryptocurrencies, promoted by the Council of Europe's Guide. Moreover, the regional workshop was an occasion to develop on the concepts of interagency cooperation, domestic Standard Operating Procedures (SOPs) and training on the search, seizure, and confiscation of online crime proceeds. The participants briefly introduced their capacities and challenges when dealing with cryptocurrencies." READ MORE

Source: Child Rescue Coalition

Date: Feb 2021

Why Facebook's plan to use end-to-end encryption is a direct threat to millions of children worldwide

"The internet has revolutionized the world but it has also a dark side and the abuse of children facilitated by technology has reached epidemic proportions. If companies like Facebook implement plans for end-to-end encryption, they will put millions of children's lives and safety at risk. […] this move to give users privacy will hamper law enforcement's ability to track and prosecute child predators on this giant social media network. […] law enforcement must be allowed to properly investigate the sexual abuse of children. This includes, when absolutely necessary, the invasion of the privacy of these highly dangerous individuals. […]" READ MORE

Source: Network and Distributed Systems Security (NDSS) Symposium 2021

Date: 25 Feb 2021

From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR

"In this study, we report the first large-scale measurement study to answer these questions, in hopes of guiding the enforcement of the GDPR and identifying pitfalls during compliance. This study is made possible by analyzing a collection of 1.2 billion WHOIS records spanning two years. […] Our findings of WHOIS GDPR compliance are multi-fold. To highlight a few, we discover that the GDPR has a profound impact on WHOIS, with over 85% surveyed large WHOIS providers redacting EEA records at scale. Surprisingly, over 60% large WHOIS data providers also redact non-EEA records. A variety of compliance flaws like incomplete redaction are also identified. The impact on security applications is prominent and redesign might be needed. We believe different communities (security, domain and legal) should work together to solve the issues for better WHOIS privacy and utility." READ MORE

Source: OSCE

Date: 25 Feb 2021

Cyber-attacks on online media endanger media freedom in BiH

"Following the recent hacker attacks on media portals Žurnal and Buka, the OSCE Mission to BiH, the European Union Delegation and European Union Special Representative, the Embassy of the United Kingdom, the Embassy of the United States, and the Office of the High Representative call on authorities in BiH to investigate all attacks on media websites as they represent a clear danger to media freedom. Cyber-attacks such as these hinder free media and the free flow of information, which are essential components of any democratic society. Government has a responsibility to protect freedom of the press." READ MORE

Source: Security Affairs

Date:24 Feb 2021

Ukraine: nation-state hackers hit government document management system

"Ukraine 's government attributes a cyberattack on the government document management system to a Russia-linked APT group. The Ukraine 's government blames a Russia-linked APT group for an attack on a government document management system, the System of Electronic Interaction of Executive Bodies (SEI EB). According to Ukrainian officials, the hackers aimed at disseminating malicious documents to government agencies. […] According to Ukraine's National Security and Defense Council, attackers acted to conduct "the mass contamination of information resources of public authorities."" READ MORE

Source: Ouest France I

Date: 24 Feb 2021

Piratage informatique. Les données médicales de 300 000 Bretons en pâture sur le dark web

Le "23 février, on apprenait le piratage massif des données médicales de 500 000 personnes en France. Ce mercredi, le hacker éthique rennais, Clément Domingo annonce avoir découvert sur le dark web 300 000 dossiers médicaux confidentiels de patients bretons, dont ceux de près de 50 000 rennais. Noms, prénoms, adresses, données médicales… Une mine d'or pour les cybercriminels et escrocs." READ MORE

Source: The Guam Daily Post

Date: 24 Feb 2021

'Draconian' moves to control internet in Asia

"From Cambodia to India […], countries in Asia have introduced a slew of internet and data use legislation in recent months, with human rights groups warning the measures raise the risk of mass surveillance and free speech violations. More than six nations have launched contact tracing systems during the pandemic – mostly without adequately safeguarding data privacy and security, campaigners say, and there have been numerous internet shutdowns and content blocks on social media and websites." READ MORE

RELATED ARTICLES

VOA News, Plan for Cyber Volunteers to Police India's Internet Draws Criticism, 25 Feb 2021

The Tribune India, India needs a dedicated cyber security law, 24 Feb 2021

Source: US Department of Justice

Date: 17 Feb 2021

Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the world

"The indictment alleges a broad array of criminal cyber activities undertaken by the conspiracy, in the United States and abroad, for revenge or financial gain. The schemes alleged include: Cyberattacks on the Entertainment Industry", "Cyber-Enabled Heists from Banks", "Ransomware and Cyber-Enabled Extortion", "Creation and Deployment of Malicious Cryptocurrency Applications", "Targeting of Cryptocurrency Companies and Theft of Cryptocurrency", "Spear-Phishing Campaigns", "Marine Chain Token and Initial Coin Offering". […] This case is a particularly striking example of the growing alliance between officials within some national governments and highly sophisticated cyber-criminals. […] With victims strewn across the globe, this case shows yet again that the challenge of cybercrime is, and will continue to be, a struggle that can only be won through partnerships, perseverance, and a relentless focus on holding criminals accountable." READ MORE

Source: US Department of Justice

Date: 16 Feb 2021

Nigerian National Sentenced to Prison for $11 Million Global Fraud Scheme

"Through subterfuge and impersonation, Obinwanne Okeke engaged in a multi-year global business email and computer hacking scheme that caused a staggering $11 million in losses to his victims." He "operated a group of companies […] based in Nigeria and elsewhere. From approximately 2015 to 2019, Okeke and others engaged" also "in other forms of cyberfraud […]" READ MORE

Source: Cámara de Diputados de México

Date: 26 Feb 2021

Análisis de la reforma a la Constitución Política de los Estados Unidos Mexicanos en materia de Ciberseguridad

"Fundamental, sancionar a ciberdelincuentes: El vicepresidente del Grupo de Trabajo de Ciberseguridad de la Coparmex, Óscar Lira Arteaga, consideró importante emprender la protección del acceso de la información y de la publicación de las ideas, así como sancionar a los ciberdelincuentes, toda vez que "hoy no se tiene el sustento para poder perseguirlos, no se tiene legislación y ello nos impide adherirnos al convenio de Budapest. […] Las amenazas no solamente son externas, la vigilancia puede ser útil para la atención de delitos, pero también puede provenir desde el mismo Estado. Por lo tanto, es fundamental establecer mecanismos de control, transparencia y rendición de cuentas para evitar abusos de vigilancia estatal." READ MORE

RELATED ARTICLES

Crónica, Plantean una reforma en ciberseguridad que proteja al usuario de internet, 26 Feb 2021

Source: Jamaica Information Service

Date: 19 Feb 2021

Jamaica: Legislation to Protect Personal Information Being Prioritised

"The Government is prioritising legislation to deal with cybercrime and to safeguard the privacy and personal information of Jamaicans, during the upcoming fiscal year. These include implementation of the Data Protection Act and promulgation of Data Protection Regulations, as well as drafting Regulations under the Telecommunications Act. A review of the Cybercrimes Act will also be undertaken." READ MORE

Source: El Peruano

Date: 23 Feb 2021

Perú: Mejoran la investigación fiscal contra el ciberdelito

"En respuesta al aumento de la ciberdelincuencia en el país, el Ministerio Público inició las labores de su nueva unidad fiscal especializada en ciberdelincuencia, que además forma parte de los compromisos asumidos por el Perú con la firma del Convenio de Budapest. [...] Según el Ministerio Público, desde el 22 de octubre del 2013 al 31 de julio del 2020 ingresaron a las fiscalías penales comunes especializadas y fiscalías mixtas 21,687 denuncias por delitos informáticos." READ MORE

Source: Ministério Público Federal

Date: 25 Feb 2021

Brazil: Workshop sobre provas eletrônicas e crimes cibernéticos promovido por MPF e OEA capacita 100 pessoas

"A Secretaria de Cooperação Internacional (SCI) e o Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do Ministério Público Federal (MPF) realizaram, nesta quinta-feira (25), a abertura do workshop Cibersegurança: Provas Eletrônicas e Crimes Cibernéticos. [...] Nesta última edição do curso, o foco são dois temas: os fundamentos básicos do tratamento da prova eletrônica, [...], e a Convenção de Budapeste, assunto tratado por Pedro Verdelho, coordenador do gabinete de Cibercrime do Ministério Público de Portugal." READ MORE

Source: Guardiana

Date: 22 Feb 2021

Cinco problemas ponen trabas a la lucha contra el cibercrimen en Bolivia

"Un Diagnóstico del Cibercrimen en Bolivia desnuda las deficiencias generales en el combate a los delincuentes informáticos. […] Solo dos delitos informáticos son sancionados por el Código Penal": "Artículo 363 bis. Manipulación informática", "Artículo 363 ter. Alteración, acceso y uso indebido de datos informáticos". "Se sugiere hacer ajustes a la legislación nacional, recurrir a la cooperación internacional y potenciar a la Policía. […] El combate contra los delitos informáticos en Bolivia tropieza al menos con cinco problemas que le restan eficacia: la falta de acceso a la información, la deficiencia en la capacitación de las autoridades, la debilidad de la legislación nacional, la falta de cooperación internacional y la carencia de personal policial especializado." READ MORE

Source: Ifex

Date: 23 Feb 2021

Digital rights in Tanzania, Uganda and Kenya throttled by COVID-19 regulations

"The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) researched Covid-19 related censorship and surveillance practices and related regulatory responses in Kenya, Tanzania and Uganda that affected peoples' digital rights, including the right to freedom of expression, access to information, and privacy. It shows that the different measures adopted by the three countries, including enactment and enforcement of repressive laws on misinformation/fake news, as well as intimidation, arrests, detentions, and suspension of media operations, have led to an erosion of civil liberties online and offline." READ MORE

Source: TeluguStop

Date: 24 Feb 2021

Zambia's Proposed Cybersecurity Bill Stirs Up Controversy

"The decision by the Zambian government to introduce a cybersecurity bill has received mixed reactions from the cross section of the society. […] Among the contentious provisions in the bill include monitoring and interception of electronic communication as well as any other information using the internet. […] A consortium of civil society organizations has since urged lawmakers to take into consideration the concerns from stakeholders. While acknowledging the need to ensure the safety of the public against cybersecurity threats, the organizations feel that this needs to be balanced with the right to freedom of expression and the need to maintain the right to privacy." READ MORE

Source: AfricaFeeds

Date: 28 Feb 2021

Ghana approves new law to jail publishers of nude pictures

"Ghana has approved a new law that seeks to punish persons who publish indecent images especially of children and women online. The new law under the country's Cybersecurity Act 2020 is an attempt to crackdown on taking and circulating or publishing of naked and sexual images of people. […] The law punishes cyber activities involving sexual abuse of children and adults – including child grooming for sexual abuse or aiding and abetting same or cyberstalking of a child with five to 15 years in jail." READ MORE

Source: University of Cape Town

Date: 25 Feb 2021

SMMEs in sub-Saharan Africa hit hard by cybercrimes

"Small, medium and micro enterprises (SMMEs) in sub-Saharan Africa have faced a range of cybersecurity issues in the wake of the COVID-19 pandemic, with scaling digital capacity exposing SMMEs to threats like ransomware, phishing and supply chain attacks. […] when many SMMEs moved to cloud-based services in response to restrictions brought on by the pandemic, cybercriminals responded with a 630% increase in cloud services attacks between January and April 2020. Other attacks included spear phishing […], ransomware, smishing (a form of phishing that involves a text message or phone number) and supply chain attacks." READ MORE

Source: BusinessTech

Date: 25 Feb 2021

These are the online and privacy changes coming to South Africa

"One of the key legal developments that South Africans should be aware of relates to information privacy and the Protection of Personal Information Act (POPIA) […] Cybercrimes Bill is also awaiting presidential signature and could come into force in 2021. Once the Bill is signed into law, a person found guilty of a cybercrime may be imprisoned for up to 15 years, depending on the offence. […] Cybercrimes include illegally accessing a computer system or intercepting data, cyber fraud, cyber forgery and cyber extortion" READ MORE

RELATED ARTICLES

ENSafrica, An Overview of the Cybercrime Bill, 18 Feb 2021

Source: ZD Net

Date: 26 Feb 2021

Cybercrime groups are selling their hacking skills. Some countries are buying

"Cyber-criminal hacking operations are now so skilled that nation-states are using them to carry out attacks in an attempt to keep their own involvement hidden. […] Not only does the client nation state end up gaining the access they require to hacked networks or sensitive information, it allows it to be done with a reduced chance of it being linked back to the nation state […]." READ MORE

Source: Ars Technica

Date: 23 Feb 2021

The bitcoin blockchain is helping keep a botnet from being taken down

"Recently, a botnet that researchers have been following for about two years began using a new way to prevent command-and-control server takedowns: by camouflaging one of its IP addresses in the bitcoin blockchain. […] By having a server the botnet can fall back on, the operators prevent the infected systems from being orphaned. Storing the address in the blockchain ensures it can never be changed, deleted, or blocked, as is sometimes the case when hackers use more traditional backup methods. […] "In this case, they're utilizing a decentralized system. You can't take it down. You can't censor it. It's there. […] While Akamai researchers say they have never before seen a botnet in the wild using a decentralized blockchain to store server addresses, they were able to find this research that demonstrates a fully functional command server built on top of the blockchain for the Ethereum cryptocurrency ." READ MORE

Source: ZD Net

Date: 25 Feb 2021

This chart shows the connections between cybercrime groups

"Cybersecurity reports often talk about threat actors and their malware/hacking operations as self-standing events, but, in reality, the cybercrime ecosystem is much smaller and far more interconnected than the layperson might realize. Cybercrime groups often have complex supply chains, like real software companies, and they regularly develop relationships within the rest of the e-crime ecosystem to acquire access to essential technology that enables their operations or maximizes their profits." READ MORE

Latest reports

- Consejo Europeo, Ciberseguridad: cómo la UE combate las amenazas cibernéticas, 22 Feb 2021
- Conselho Europeu, Cibersegurança: como combate a UE as ciberameaças, 22 Feb 2021
- Coindesk, Russia and US Dominate Global Dark Market Traffic, 2 Feb 2021
- Malwarebytes, State of Malware report 2021, 16 February 2021
- TechNewsWorld, The Future of Cybersecurity in 2021 and Beyond, 16 Feb 2021
- Varonis, 134 Cybersecurity Statistics and Trends for 2021, 22 Feb 2021
- UNODC, Darknet Cybercrime Threats to Southeast Asia, 25 Feb 2021
- Anti-Cybercrime Group, ACG-CYBER SECURITY BULLETIN NR 203: Understanding the Risk of Trojan Malware, 19 Feb 2021
- MyBroadband, How much your private data sells for on the dark web, 26 Feb 2021
- Yahoo!Finance, Crypto price surge invites a torrent of crypto crime, 20 Feb 2021
- Security Magazine: Cybercrime report finds young adults and adults over 75 most vulnerable to fraud attacks, 25 Feb 2021
- InsuranceBusiness, What is actually fuelling cybercrime?, 23 Feb 2021

Upcoming events

- 1-5 March, C-PROC/INTERPOL (on-line), INTERPOL Malware Analysis Training (Africa, Europe and Middle East), GLACY+
- 2 March, ASEAN, (on-line), Participation in "Building Anti-Cybercrime Capacity in ASEAN for the Equality, Diversity and Inclusion (EDI) toolkit" organized by Chatham House, GLACY+
- 2-3 March, C-PROC/TRINIDAD AND TOBAGO, (online), Workshop on Cybercrime legislation in Trinidad and Tobago, Octopus project in cooperation with CARICOM IMPACS
- 3 March, C-PROC, (on-line), African DPAs Network Series of Regional Webinars (5th workshop), GLACY+
- 3-5 March, C-PROC/AZERBAIJAN, (on-line), Development of standard operating procedures for cooperation between CSIRTs and law enforcement (with CyberSecurity EAST project), CyberEast
- 4 March, C-PROC/THAILAND, (on-line), Participation in "Applying data protection rules in criminal proceedings" organized by U.S. Department of Justice, GLACY+
- 4-5 March, C-PROC/LEBANON, (on-line), 2nd Workshop for mainstreaming the judicial training, CyberSouth
- 4-5 March, C-PROC/ARMENIA, (on-line), Workshop with personal data protection authorities and national communications regulators on trust and cooperation, CyberEast
- 8 March, C-PROC/LEBANON, (on-line), 3rd Workshop for the development of domestic Standard Operational Procedures on e-evidence, CyberSouth
- 9 March, Ancillary meeting "Cooperation on cybercrime: risks and safeguards" at the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice, T-CY and Octopus project
- 9 March, C-PROC/Children's Rights Division, (on-line), Webinar Cyber-bullying: trends, prevention strategies and the role of law enforcement, Joint activity EndOCSEA@Europe and iProceeds2.

- 9-10 March, C-PROC/BARBADOS, (online), Workshop on Cybercrime legislation in Barbados, Octopus project in cooperation with CARICOM IMPACS
- 9-11 March, C-PROC/CAPE VERDE, (on-line), Support to the national delivery of Introductory Course on cybercrime and electronic evidence for judges and prosecutors, GLACY+
- 9-11 March, C-PROC/ARMENIA, (on-line), Effective access to data exercise and development of standard procedures between LEA/ISPs, CyberEast
- 10 March, C-PROC/PHILIPPINES, (on-line), Advisory mission on developing/adapting the training materials for on-line basic modules, GLACY+
- 11 March, C-PROC/BELIZE, (on-line), Stakeholder webinar on new cybercrime legislation, GLACY+
- 12 March, C-PROC/NIGERIA, Desk study on cybercrime legislation and human rights, GLACY+
- 12 March, C-PROC/TUNISIA, (on-line), 3rd Workshop for mainstreaming the judicial training, CyberSouth
- 15-18 March, C-PROC/ARMENIA, (on-line), Pilot session of online judicial training, CyberEast