Cybercrime Digest

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

16 – 31 January 2021

Source: Council of Europe

Date: 16 Jan 2021

Data Protection Day: 40 years of Convention 108

"Forty years ago tomorrow, on 28 January 1981, the first ever binding international treaty addressing the need to protect personal data was opened for signature in Strasbourg: the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as "Convention 108". The treaty was modernised in 2018 by an Amending Protocol, not yet in force, aimed at ensuring that its data protection principles are still adapted to new technologies and to strengthen its follow-up mechanism. […] Open to any country and with the unique potential to become a global standard, in 1981 the "Convention 108" established the basic principles of data protection and rules which are still applicable today. Drafted in a technologically neutral style, the convention has remained fully valid for four decades. Today it has 55 state parties in four continents – another 20 countries participate in its work - and the Convention has become the backbone of national legislation in many countries throughout the world." READ MORE

Source: Human Rights Watch

Date: 16 Jan 2021

Proposed UN Cybercrime Treaty Could Undermine Human Rights

"[…] In recent years, Russia has significantly expanded laws and regulations tightening control over internet infrastructure, online content, and the privacy of communications. A UN cybercrime convention could severely undermine the ability of people to exercise their human rights online, including freedom of expression and freedom of access to information, if it's modeled after Russia's domestic approach to internet policy. The controversial UN resolution that set this process in motion is exceedingly vague in how it defines cybercrime. In many countries, legislation and policies aimed at combating cybercrime use vague and ill-defined terms to criminalize legitimate forms of online expression, association, and assembly. These give wide-ranging power to governments to block websites deemed critical of the authorities, or even entire networks, applications, and services that facilitate online exchange of and access to information." READ MORE

Source: Council of Europe

Date:29 Jan 2021

Plenary meeting kicks off the International Network of the National Judicial Trainers on cybercrime and electronic evidence

"Following the commitment expressed during the second meeting of the International Network of the National Judicial Trainers on Cybercrime and Electronic Evidence ("the Network"), on 29 January 2021, GLACY+, iPROCEEDS-2, CyberSouth and CyberEast Projects, organized the on-line plenary meeting of the Network, to discuss over the Terms of Reference of the Network and 2021 workplan. During the workshop, participating members agreed on the use of terms of reference as the rules for operating the Network. A short term action plan for 2021 and a workplan for 2021 have been discussed and agreed. As a concrete outcome, a series of monthly practitioners-to-practitioners workshops are envisaged to be designed and delivered by the members of the Network to their peers." READ MORE

Source: Europol

Date: 27 Jan 2021

World's most dangerous malware EMOTET disrupted through global action

"Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action. This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). EMOTET has been one of the most professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years. The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this unauthorised access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware." READ MORE

Source: European Commission

Date: 20 Jan 2021

EU Internet Forum Ministerial: towards a coordinated response to curbing terrorist and child sexual abuse content on the internet

"The Forum gathered EU Member States, industry, academia, law enforcement, European agencies and international partners to discuss and address the challenges posed by the presence of malicious content online. In the course of today's video-conference, participants had the possibility to exchange views on several issues: EU and industry response to recent terrorist attacks in France and Austria, including the Europol report on the activation for the first time of the EU Crisis Protocol, a voluntary mechanism to help coordinate a rapid, collective and cross-border response to the viral spread of terrorist and violent extremist content online. […] Emerging challenges such as the threats posed by Violent Right-Wing Extremism's online content. […] The Commission presented the outcomes of an expert consultation process to identify technical solutions that could allow companies to detect child sexual abuse in end-to-end encrypted electronic communications." READ MORE

Source: ENISA

Date: 20 Jan 2021

Training Together to Fight Cybercrime: Improving Cooperation

"The European Union Agency for Cybersecurity releases a new report and training material to support the cooperation among CSIRTs, Law Enforcement Agencies (LEAs) and their interaction with the judiciary. The publications are designed to help tackle the challenges of this complex multi-stakeholder cooperation. The report, the handbook and the toolset are a set of deliverables complementing each other as follows: (i) The report analyses roles, duties, competences, synergies and potential interferences across Computer Security Incident Response Teams (CSIRTs) - in particular, national and governmental ones, LE and judiciary (prosecutors and judges); (ii) The handbook helps a trainer explain these concepts through different scenarios; (iii) The toolset consists of exercises meant for trainees based on the handbook's scenarios." READ MORE

Source: Council of Europe

Date:27 Jan 2021

Romania – Brazil bilateral meeting on best practices of the 24/7 POC under the Budapest Convention

"Within the framework of the Global Action on Cybercrime Extended Project (GLACY+), Brazilian officials met today in a virtual meeting with the representatives of the Directorate for Investigating Organized Crime and Terrorism of the Romanian General Prosecutor's Office and the Cybercrime Unit of the Romanian National Police, to discuss on "Establishment and internal coordination of the 24/7 point of contact under the Budapest Convention […] Brazil has been invited to accede to the Budapest Convention in 2019 and the establishing of a functioning 24/7 point of contact is one of the requirements to be fulfilled when depositing the instruments of accession. Furthermore, Brazil will be included this year in the list of GLACY+ priority countries and will receive full support from the project to strengthen capacities of criminal justice authorities in the fight against cybercrime." READ MORE

Source: INTERPOL

Date: 22 Jan 2021

INTERPOL report charts top cyberthreats in Southeast Asia

"INTERPOL's ASEAN Cyberthreat Assessment 2021 report outlines how cybercrime's upward trend is set to rise exponentially, with highly organized cybercriminals sharing resources and expertise to their advantage. It provides strategies for tackling cyberthreats against the context of the pandemic which has seen more people going online using mostly unprotected mobile devices, creating a surge in cybercriminal activities profiting from the theft of personal information and credentials. The report further describes the essential collaboration on intelligence sharing and expertise between law enforcement agencies and the private sector, facilitated by INTERPOL's global network." READ MORE

RELATES ARTICLES

The Interpreter, Filling the gaps in ASEAN and EU cybercrime cooperation, 1 Feb 2021

The Strategist, ASEAN needs to enhance cross-border cooperation on cybercrime, 19 Jan 2021

Source: Europol

Date: 20 Jan 2021

France arrests 14 suspects in sweep against child sexual abuse online

"A nation-wide operation led by the French Gendarmerie (Gendarmerie nationale) with the support of Europol that targeted suspects who sexually exploited children online has netted 14 arrests. Code-named 'Horus' the operation took place between 16 and 20 November 2020. The alleged suspects used social media networks to approach minors aged between 12 and 13 and lured them into sharing intimate images and videos. The arrested suspects are said to have had no links between them and three have already been sentenced. With investigations still ongoing, operation Horus has contributed to identifying eight potential victims and the seizure of 1 058 illicit images." READ MORE

RELATED ARTICLES

Business Insider, Online child sex abuse spiked by 31% in 2020, with at least 13 million disturbing images on Facebook and Instagram, 21 Jan 2021

Source: CircleID

Date: 19 Jan 2021

WHOIS Record Redaction and GDPR: What's the Evolution Post-2018?

"Despite WHOIS's relevance, however, the dawn of new data regulations like the General Data Protection Regulation (GDPR) seemingly disconnected the ties that bind domains to their owners. While it's true that the data contained in WHOIS records can be partly personal, it does serve a crucial purpose when determining who or what outfit could be responsible for a cyber attack. We sought to quantify the extent of the implications of WHOIS record redaction in this report and summarize our key findings here." READ MORE

RELATED ARTICLES

Interisle, Interisle Study Reveals Excessive Withholding of Internet Whois Data, 25 Jan 2021

Source: U.S. Department of Justice

Date: 27 Jan 2021

Global Action against NetWalker Ransomware: Defendant Charged, Dark Web Resource Disabled, Nearly $500,000 Seized

"The Department of Justice today announced a coordinated international law enforcement action to disrupt a sophisticated form of ransomware known as NetWalker. NetWalker ransomware has impacted numerous victims, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities. Attacks have specifically targeted the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims. […] According to court documents, NetWalker operates as a so-called ransomware-as-a-service model, featuring "developers" and "affiliates." Developers are responsible for creating and updating the ransomware and making it available to affiliates. Affiliates are responsible for identifying and attacking high-value victims with the ransomware, according to the affidavit. After a victim pays, developers and affiliates split the ransom." READ MORE

Source: INTERPOL

Date: 19 Jan 2021

INTERPOL, Investment fraud via dating apps

"INTERPOL has issued a Purple Notice to its 194 member countries outlining a specific modus operandi on dating applications. The threat involves taking advantage of people's vulnerabilities as they look for potential matches, and luring them into a sophisticated fraud scheme. In the initial stages, an artificial romance is established via a dating app. Once communication becomes regular and a certain level of trust is established, criminals share investment tips with their victims and encourage them to join a scheme." READ MORE

Source: Diario Futrono

Date: 24 Jan 2021

Chile: Despachan a Sala proyecto que adecua legislación sobre delitos informáticos

"Con la aprobación de una serie de modificaciones consensuadas con equipos multisectoriales, la Comisión de Futuro, Ciencias, Tecnología, Conocimiento e Innovación, aprobó y despachó a la Sala, el proyecto de ley que establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest (boletín 12.192)." READ MORE

Source: Citi Newsroom

Date: 28 Jan 2021

What Ghana should learn as we mark international Data Protection and Privacy day

"[…] Cyber Security and National Security go hand in hand. Cyber intelligence operations must be considered as an integral part of the national security set up. This should not be focused on only cybercriminals but possible intrusions and attacks by nation-states as well. Cyber has become a means of espionage by many advanced and superpower countries across the globe to spy on other countries, which ultimately threatens the national security and sovereignty of those countries." READ MORE

Source: New Era

Date: 28 Jan 2021

Data protection and privacy in Namibia through Covid-19 lenses

"Although Namibia is known for upholding rule of law, the country does not have a data protection and privacy law in place. The wake of the Covid-19 pandemic, in particular, has highlighted the importance of the data protection law as incidents of data violations and breaches became prominent." READ MORE

Source: Hindustan Times

Date: 29 Jan 2021

India, no clear definition, computer-aided offence a cybercrime: Minister of Home Affairs' report

"The Union home ministry, in its report submitted to the Parliamentary panel on Home Affairs, has said that even as there is no "legislative definition for cybercrime", any offence committed "against a computer resource or with the aid of a computer resource is called a cybercrime". "Such offences are dealt as per the legal provisions of the Information Technology Act, Indian Penal Code, POSCO etc," the ministry has said. It added that government has also straightened the legal framework by dealing with cybercrime cases against women and children as child sex abuse materials. Last year, the government rolled out the Cyber Crime prevention against Women and Children scheme, with an online cybercrime reporting platform." READ MORE

Source: Euronews

Date: 27 Jan 2021

Romania criminalises creating fake social media accounts

"It's a criminal offence to create a fake social media account in the name of another person, a court in Romania has ruled. Opening an account that looks like someone else without their consent is a "crime of forgery", said the High Court of Cassation and Justice, the country's panel for resolving legal issues in criminal matters. It comes after a case in Braşov in December 2018 where a man had threatened his former girlfriend with uploading compromising photos." READ MORE

Source: Foreign Policy

Date: 24 Jan 2021

The World Needs a Cyber-WHO to Counter Viruses in Cyberspace

"Imagine if only a dozen or so nations were able to diagnose COVID-19, understand how it spread, the damage it could cause, and how to prevent and treat it. In addition, these privileged nations kept that information to themselves. This is, effectively, the situation we have with cybersecurity. Virtually all countries are at a higher risk of attack because of their inability to identify their attackers, to say nothing of defending themselves and remediating the damage." READ MORE

Latest reports

- European Commission, Fighting cybercrime, 31 Jan 2021
- European Commission, EU Cybersecurity Strategy - A brochure, 28 Jan 2021
- ENISA, Cybersecurity to the Rescue: Pseudonymisation for Personal Data Protection, 28 Jan 2021
- World Economic Forum, These are the top cybersecurity challenges of 2021, 21 Jan 2021
- Europol, The Use of Violence by Organised Crime Groups, 29 Jan 2021
- The Africa Report, Three ways West Africa's digitalisation can improve, 28 Jan 2021
- Africa Center for Strategic Studies: Africa's Evolving Cyber Threats, 19 Jan 2021
- Ministerio Publico Federal do Brasil, Combate às fraudes no auxílio emergencial e fortalecimento dos acordos de não persecução penal marcam atuação da Câmara Criminal do MPF em 2020, 20 Jan 2021

Upcoming events

- 1-3 February, C-PROC/Moldova, (on-line), Training on international cooperation on cybercrime and electronic evidence, CyberEast
- 3 February, C-PROC/Strasbourg, (on-line), African DPA Network Series of Regional Webinars (4th workshop), GLACY+
- 3 February, C-PROC/Morocco, (on-line), National Workshop on the preparation of cybercrime and e-evidence situation (annual) report, CyberSouth, GLACY+
- 3-4 February, C-PROC/ Kosovo*, (on-line), Business analysis CERT/LEA, iPROCEEDS-2
- 3-4 February, C-PROC/Kosovo*, (on-line), Guidelines and procedures on sharing of data by CERTs/CSIRTs with criminal justice authorities, iPROCEEDS-2
- 4-5 February, C-PROC/Georgia, (on-line), Workshop with personal data protection authorities and national communications regulators on trust and cooperation, CyberEast
- 5 February, C-PROC/Morocco, (on-line), National Workshop on Standard Operating Procedures, CyberSouth, GLACY+
- 8-10 February, C-PROC/Armenia (on-line), Training on international cooperation on cybercrime and electronic evidence, CyberEast
- 8 February, C-PROC/Serbia, (on-line), Meeting on the assessment of the collection and investigation/ handling of electronic evidence, iPROCEEDS-2
- 10 February, C-PROC, (on-line), Regional workshop for representatives of judicial training academies to review the current state of judicial training and agree on project approach, iPROCEEDS-2
- 15-16 February, C-PROC/ Moldova (on-line), Workshop with personal data protection authorities and national communications regulators on trust and cooperation, CyberEast
- By 15 February, C-PROC/Strasbourg, (on-line), T-CY: Support of the T-CY work on negotiation of a 2nd Additional Protocol to the Budapest Convention, T-CY, Octopus Project
- By 15 February, C-PROC/Strasbourg, (on-line), Preparation of country profiles on online child sexual exploitation and abuse, Octopus Project, EndOCSEA@Europe
- By 15 February, C-PROC, Initiation of the desk review of the national legislation on cybercrime and electronic evidence in the Caribbean region, Octopus Project in cooperation with CARICOM IMPACS.

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.