Cybercrime Digest

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

01 – 15 May 2021

Source: Council of Europe

Date: 13 May 2021

International Association of Prosecutors and Council of Europe focus on the Second Additional Protocol: Enhanced Cooperation and Disclosure of E-Evidence

"Between May and December 2021, the International Association of Prosecutors and the Council of Europe, through GLACY+ and Octopus projects, are co-organising a series of thematic webinars to exchange views on the existing and emerging forms of cooperation for effective access to electronic evidence, as well as solutions proposed by the 2nd Additional Protocol to the Convention on Cybercrime on enhanced international cooperation and disclosure of electronic evidence. During the first webinar that took place on 13 May, the panelists discussed about the challenges of direct cooperation with service providers and other entities and presented the solutions offered by the Second Additional Protocol for obtaining domain name registration information and for disclosure of subscriber information, with emphasis on the novel direct order to a service provider in another Party." READ MORE

Source: CyberScoop

Date: 05 May 2021

UN cybercrime proposal could help autocrats stifle free speech, rights group says

"Human rights advocates are warning that a controversial proposal at the United Nations to counter cybercrime could validate tactics that autocratic governments around the world have used to criminalize free speech and security research. The Russian and Chinese governments back the notion of establishing a new anti-cybercrime convention, a process that diplomats at the U.N. will begin considering next week. However, the wording of the proposal, which calls for curbs on the use of technologies for "criminal purposes," is vague to the point of potentially enabling further government repression, critics say." READ MORE

Source: ZDNet

Date: 13 May 2021

Colonial Pipeline attack: Everything you need to know

"The real-world consequences of a successful cyberattack have been clearly highlighted this week with the closure of one of the US' largest pipelines due to ransomware. Here's everything we know so far. On Friday, May 7, Colonial Pipeline said that a cyberattack forced the company to proactively close down operations and freeze IT systems after becoming the victim of a cyberattack. This measure "temporarily halted all pipeline operations" and cybersecurity firm FireEye, which operates the Mandiant cyberforensics team, was reportedly pulled in to assist. […] As a group known to double-extort victims, Colonial Pipeline could be the next company to face the threat of the leak of data unless they give in to blackmail and pay the attackers. It may be, however, that DarkSide could choose not to pursue this usual tactic due to the aforementioned "social" problems caused by the ransomware. Bloomberg says that during the attack, over 100GB in corporate data was stolen in just two hours. As of May 11, Colonial Pipeline has not been added to the DarkSide leak site. On May 13, Bloomberg reported that the company paid a ransom demand of close to $5 million in return for a decryption key. This appears to be one of the largest and most successful cyberattacks on a critical component of a country's infrastructure to date" READ MORE

Source: CyberScoop

Date: 05 May 2021

USA: CISA used new subpoena power to contact US companies vulnerable to hacking

"[…] Congress granted CISA the subpoena power in a bill that became law in January, allowing the agency to obtain a list of an internet service provider's vulnerable customers and notify them directly rather than relying on third party communication. CISA issued two such subpoenas last week, acting agency director Brandon Wales said. A CISA spokesperson declined to say which U.S. company or companies had been subpoenaed, or whether the vulnerabilities pertained to an ongoing hacking campaign." READ MORE

RELATED ARTICLE:

Schneier on Security, New US Executive Order on Cybersecurity, 13 May 2021

Source: EU Reporter

Date: 11 May 2021

The European Commission makes 11 million EURO available to strengthen cybersecurity capabilities and co-operation

"The European Commission will make €11 million of funding available for 22 new projects seeking to strengthen the European Union's capacity to deter and mitigate cyber-threats and incidents, by employing the latest technologies. The projects, which have been selected following a recent call for proposals under the Connecting Europe Facility programme, will support various cybersecurity organisations in 18 Member States." READ MORE

RELATED ARTICLE:

Euractiv, EU and French cybersecurity heads call for greater cooperation, extra resources, 7 May 2021

Source: Europol

Date: 03 May 2021

4 Arrested in takedown of dark web child abuse platform with some half of a million users

"Four have been arrested in a multi-agency operation sparked by a German investigation into one of Europe's most prolific child sexual abuse platforms on the dark web.[…] The dark web platform, known as Boystown, has been taken down by an international taskforce set up by the German Federal Criminal Police (Bundeskriminalamt) which included Europol and law enforcement agencies from the Netherlands, Sweden, Australia, Canada and the United States." READ MORE

RELATED ARTICLE:

Europol, New trace an object uploads: fresh leads needed in child sexual abuse cold cases, 10 May 2021

Source: Council of Europe

Date: 04 May 2021

Japan makes a voluntary contribution to support the action against cybercrime

"The Government of Japan has made a voluntary contribution of €151,754 to support the Council of Europe action against cybercrime, and notably to assist Asian countries in strengthening the criminal justice response to Covid-19-related cybercrime. Ambassador Takeshi Akamatsu, Permanent Observer of Japan to the Council of Europe, met with Mr Bjørn Berge, Deputy Secretary General, on this occasion."

Source: CyberPeace Institute

Date: 12 May 2021

WannaCry is Not History

"May 12 marks the fourth anniversary of the WannaCry ransomware attack, ominously named after the *.wncry* extension it adds to the files it encrypts. Within 24 hours of its detection, the ransomware had spread to around 150 countries, roasting thousands of computers in over 200,000 organizations.[…] The first lesson to be learned in the aftermath of WannaCry is that identifying and charging those responsible takes a considerable amount of time, consequently exacerbating the impact of the attack on targets and victims." READ MORE

Source: ZD Net

Date: 05 May 2021

Belgium: Massive DDoS attack took large sections of a country's internet offline

"A massive distributed denial of service (DDoS) attack took down the websites of more than 200 organisations across Belgium […]. Belgium's central authority for cybersecurity, the Center for Cybersecurity Belgium (CCB), was contacted following the attack in order to help contain and resolve it. One of the reasons the attack was so disruptive was because those behind the disruption kept altering the techniques behind it." READ MORE

Source: Euractiv

Date: 11 May 2021

Germany sees cybercrime jump as work shifts online in pandemic

"Germany's shift towards digitalisation due to the coronavirus pandemic has come with a significant rise in cybercrime, according to a report by the country's Federal Criminal Police Office (BKA). Recorded cases of cybercrime jumped by 8% in 2020, according to the BKA's Situation Report for Cybercrime 2020 published on Monday (10 May). […] The number of solved cases fell by 7.4% over two years to 32.6% in 2020." READ MORE

Source: Irish Times

Date: 03 May 2021

Irish data watchdog clashes with regulators over proposed WhatsApp fine

"The Data Protection Commissioner has clashed with several of her European counterparts after they objected to her proposal to impose a fine of up to €50 million on WhatsApp for violating privacy laws. The row between Helen Dixon and regulators in other countries is the second dispute over a major privacy case since she took on pan-EU powers to investigate data breaches by big technology firms based in Ireland, whose websites and apps are used by hundreds of millions in Europe." READ MORE

Source: Council of Europe

Date: May 2021

CyberEast Interview: The work of the International Relations Department of the Ministry of Internal Affairs of Georgia in drafting cybercrime policies

"[…] The cybercrime investigation is becoming very complicated without proper preparation and precautions. Combating cybercrime is one of the three main objectives of Georgia's National Strategy for Combatting Organized Crime 2021-2024 and its Action Plan 2021-2022; both documents containing separate sections dedicated to cybercrime." READ MORE

Source: INTERPOL

Date: 12 May 2021

INTERPOL launches initiative to fight cybercrime in Africa

"INTERPOL is creating a new cybercrime operations desk with UK funding to boost the capacity of 49 African countries to fight cybercrime. The Africa desk will help shape a regional strategy to drive intelligence-led coordinated actions against cybercriminals and support joint operations." READ MORE

RELATED ARTICLE:

The New Times, Rwanda among five African countries at the forefront of fighting cybercrimes, 12 May 2021

Source: Threat Proof

Date: 03 April 2021

Deepfake attacks are about to surge, experts warn

"Artificial intelligence and the rise of deepfake technology is something cybersecurity researchers have cautioned about for years and now it's officially arrived. Cybercriminals are increasingly sharing, developing and deploying deepfake technologies to bypass biometric security protections, and in crimes including blackmail, identity theft, social engineering-based attacks and more, experts warn. A drastic uptick in deepfake technology and service offerings across the Dark Web is the first sign a new wave of fraud is just about to crash in, according to a new report from Recorded Future, which ominously predicted that deepfakes are on the rise among threat actors with an enormous range of goals and interests." READ MORE

Source: scidev.net

Date: 13 May 2021

Rights group launches tool to stem cybercrime in Africa

"Victims of cyberbullying and related crimes can now get redress thanks to a new online platform that seeks to empower internet users across Africa to report digital rights violations. The platform called Ripoti, a Swahili word meaning report, was launched last month at the 2021 Digital Rights and Inclusion Forum. It links victims to expert support and enables them to document and track evidence of violations. […] The new platform seeks to provide redress for violations that usually go unnoticed when not reported. It also creates awareness of the different types of violations, which ones are more prevalent and pressing, and documents these into a body of evidence that can inform advocacy intervention by various partners." READ MORE

Source: The Herald

Date: 07 May 2021

Zimbabwe: Cybercrime threat to national security

"Zimbabwe's national security is under threat from a plethora of cybercrimes that are causing havoc across the world. Urgent action is actually required because the country is vulnerable to online crimes. […] The ongoing debate on the draft Cyber Security and Data Protection Bill should be undertaken honestly and objectively. Partisan inclinations and polarisation should not stop people from objectively debating such an important piece of legislation.[…] Though not a member, Zimbabwe has done well in borrowing some aspects from both the Budapest and Malabo Conventions, for its Cyber Bill has progressive clauses that strengthen data protection, consolidate cyber-related offences and promote technology for businesses to flourish. Therefore, Zimbabwe should consider joining the Budapest Convention to enhance cooperation on cybercrime." READ MORE

Source: lavozdelgrito.com

Date: 11 May 2021

Argentina: Crearon una nueva fiscalía especializada en cibercrime y trata de personas

"Se puso en marcha la nueva Fiscalía especializada en Cibercrimen contra las Infancias y Delitos Conexos a la Trata de Personas en el Departamento Judicial de Quilmes. […] "A lo largo de los años no solo ha aumentado de manera ostensible el caudal de procesos iniciados por los delitos antes mencionados, sino que además la complejidad de la investigación de tales figuras ha generado una particular especialización del personal en conocimientos técnicos e informáticos que torna su actividad distinta de la que caracteriza la investigación de los demás delitos criminales", indicaron desde la Fiscalía en su fundamentación" READ MORE

Source: ZD Net

Date: 10 May 2021

Group pleads guilty for running bulletproof hosting service for criminal gangs, malware payloads

"[…] According to the US DoJ, the group rented out servers and domains that were used in criminal campaigns including attacks against US companies and financial organizations. […]"A key service provided by the defendants was helping their clients to evade detection by law enforcement and continue their crimes uninterrupted; the defendants did so by monitoring sites used to blocklist technical infrastructure used for crime, moving "flagged" content to new infrastructure, and registering all such infrastructure under false or stolen identities," prosecutors say." READ MORE

Latest reports

- European Data Protection Board, EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime, 04 May 2021
- ENISA Report: Recommendations for the security of CAM (Computer-Aided Manufacturing), 05 May 2021
- Circle ID, COVID-19-Related Bulk Domain Registrations: A Possible Case of DNS Abuse?, 03 May 2021
- Security.org, Data Security: 25 Important Facts & Statistics for 2021, 10 May 2021
- Trilateral Research, Young and connected: An analysis of the new General Comment on children's rights in the digital environment, 05 May 2021
- E-commerce Mag, Le risque cyber évalué à 6 000 milliards de dollars en 2021, 3 May 2021
- Verizon, Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report, 13 May 2012
- UNESCO, The Chilling: Global trends in online violence against women journalists, May 2021

Upcoming events

- 17-18 May, C-PROC/UKRAINE, (on-line), Development of Standard Operating Procedures for Cooperation between CSIRTs and Law Enforcement – Stage II (in cooperation with Cybersecurity EAST project), CyberEAST
- 18-20 May, C-PROC/ MONTENEGRO, (on-line), Specialised Judicial Training Course on International Cooperation, iPROCEEDS-2
- 20-21 May, C-PROC/GEORGIA, (on-line), Development of Standard Operating Procedures for Cooperation between CSIRTs and Law Enforcement – Stage II (in cooperation with Cybersecurity EAST project), CyberEAST
- 22 May, T-CY, Translation of the Budapest Convention and its Protocol into Amharic, Octopus
- 24 May-25 June, C-PROC/INTERPOL, (on-line), Instructor Development Course for English speaking countries, GLACY+
- 24 May, C-PROC/ MONTENEGRO, (on-line), Workshop on drafting a complex cybersecurity strategy that is in line with international standards, iPROCEEDS-2
- 25 May, C-PROC/all iPROCEEDS-2 countries, (on-line), International Webinar to officially start the training course on Python Programming for Investigators Online, iPROCEEDS-2
- 24-25 May, C-PROC/ARMENIA, (on-line), Development of Standard Operating Procedures for Cooperation between CSIRTs and Law Enforcement – Stage II (in cooperation with Cybersecurity EAST project), CyberEAST
- 25-26 May C-PROC/Children's Rights division, (on-line), Pilot training on online child sexual abuse and exploitation for judges, prosecutors and the national police in the Republic of Moldova, EndOCSEA@Europe
- 26-27 May, C-PROC/TURKEY, (on-line), Business analysis CERT/LEA, iPROCEEDS-2
- 26-27 May, C-PROC, T-CY, 10th Protocol Drafting Plenary (online), T-CY, Octopus
- 27 May, C-PROC, (on-line), Series of monthly thematic webinars for the International Network of the National Judicial Trainers, GLACY+

- 28 May, C-PROC, T-CY, 24th T-CY Plenary (online), T-CY, OctopusBy 30 May, C-PROC, Desk study, Development of new materials for the Advanced Judicial Course on Cybercrime and Electronic Evidence, GLACY+
- By 30 May (publishing date tbd) C-PROC/Children's Rights division, Desk study, Update of Member States' Responses to Prevent and Combat Online Child Sexual Exploitation and Abuse Baseline Mapping - Second Edition, EndOCSEA@Europe
- By 31 May (date TBC), C-PROC/ARGENTINA, (on-line), Support to the establishment of a regional training center on cybercrime and electronic evidence and a certification program for criminal justice authorities in Latin America, GLACY+
- By 31 May (date TBC), C-PROC/BURKINA FASO, (on-line), Advisory mission on legislation, GLACY+
- By 31 May (date TBC), C-PROC/COTE D'IVOIRE, (on-line), Advisory mission on legislation, GLACY+
- By 31 May, C-PROC, Translation (SP) of the Specialized course on International Cooperation for Prosecutors and Judges, GLACY+
- By 31 May, C-PROC, Development of research methodology for the Public Opinion Surveys in the EAP countries, CyberEAST
- By 31 May, C-PROC, Desktop Review of Introductory Training Course for Judges on cybercrime and electronic evidence (in partnership with the High School of Justice of Georgia), CyberEAST
- May/June, C-PROC, Desk analysis, Development of a Guide on Law Enforcement Training Strategies, CyberSouth, GLACY+

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 May 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