Cybercrime Digest

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

16 – 31 August 2020

Source: EU CYBER DIRECT

Date: 25 Aug 2020

EU Cyber Forum 2020 will take place online on 14 – 17 September 2020

"Over the past years, cyber-related policy issues have become a permanent feature on the meeting agendas of European leaders with third countries. With the increased focus on digital transition and the relevance of the EU's cyber and digital policies in support of the Geopolitical Commission, the EU's diplomatic, economic and political actions attract international attention and scrutiny. […]. To support these objectives and to deepen the EU's global engagement with various stakeholder communities and our strategic partners around the world, the European Union Institute for Security Studies (EUISS) and partners are organising the EU Cyber Forum (14-17 September 2020, Brussels) for the second consecutive year." READ MORE

Source: Eurojust

Date: 26 Aug 2020

New major crackdown on one of the biggest online piracy groups in the world: international coordination led by Eurojust

"An alleged criminal network of copyright infringing hackers, mainly responsible for pirating movies and hosting illegal digital contents worldwide, was dismantled yesterday in a coordinated action between US authorities and their counterparts in 18 countries around the world, with Eurojust and Europol support. Over 60 servers were taken down in North America, Europe and Asia and several of the main suspects were arrested. The alleged illegal activity was causing tens of millions of USD in losses on an annual basis mainly to the US movie, television, and supporting industries**.** Based on allegations contained in court documents, the organised crime group (OCG) called the 'Sparks Group' dismantled yesterday was one of the biggest ones in the world responsible for online piracy." READ MORE

RELATED ARTICLES

Europol, One of the biggest online piracy groups taken down, 26 Aug 2020

Source: Council of Europe

Date: 14 Aug 2020

CyberEast: Long-distance Master Programme in Cybercrime Investigation and Computer Forensics starting in September 2020

"Ten law enforcement/criminal justice officers from Eastern Partnership countries (Armenia, Belarus, Georgia, Moldova, Ukraine) will be supported through the joint European Union – Council of Europe CyberEast project to participate in the upcoming long-distance master programme MSc Forensic Computing and Cybercrime Investigation offered by the University College Dublin, Ireland. The programme will start in September 2020 and run for 24 months, covering modules such as Computer Forensics, Network Investigations, Financial Investigation Techniques – Following the Money, Mobile Devices Investigation, Programming for Investigators, Live Data Forensics, VoIP and Wireless Investigations and others." READ MORE

Source: Council of Europe

Date: 26 Aug 2020

INTERPOL E-Evidence Boot Camp completed, an 8 week-long e-learning training for GLACY+ countries

GLACY+ project participated in INTERPOL's E-Evidence Boot Camp (EEBC) courses provided between 15 June to 28 August. The EEBC is an 8-week long online training course on electronic evidence developed by INTERPOL in collaboration with University College Dublin. It combines self-paced learning, web forum and weekly online webinars where participants exchange ideas. The syllabus is compact with recorded lectures, readings and weekly assessments on key aspects of computing, information technology and digital forensics. A total of 21 participants (from Benin, Chile, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Paraguay, Philippines, Senegal) successfully completed the training together with other invited law enforcement participants. The GLACY+ Project contributed webinars on International Cooperation and the Budapest Convention during the courses.

Source: Ghana News Agency

Date: 28 Aug 2020

Ghana's first child protection digital forensic laboratory launched

"UNICEF Ghana, in collaboration with the Ghana Police Service, has launched Ghana's first ever digital forensic laboratory, designed especially to prevent and respond to criminal acts of online abuse, exploitation and violence against children. This specialized unit will strengthen the reliability and integrity of investigations of online abuse against children through the acquisition, analysis and presentation of electronic evidence from digital devices and the internet. The laboratory is the first of its kind in the West and Central African sub-regions, and will link the Ghana Police Service with Interpol's International Child Sexual Exploitation Database. Madam Anne-Claire Dufay, UNICEF Country Representative in Ghana, said the main objectives forensic lab project were to protect children and women from online violence and abuse; to provide solid evidence that could be used in judicial proceedings, to prosecute criminals; and as a result, to improve the rate of prosecutions and convictions against cyber predators." READ MORE

Source: heraldodemexico.com.mx

Date: 20 Aug 2020

México y el Convenio de Budapest

"El Convenio sobre la Ciberdelincuencia del Consejo de Europa, mejor conocido como Convenio de Budapest, es el instrumento internacional más ambicioso (el único vinculante, además) en su tipo. […] Los países integrantes armonizan sus leyes en la materia, intercambian información y se apoyan mutuamente para prevenir, investigar y sancionar crímenes cometidos a través de medios digitales. […] En México, el gobierno ya ha sido objeto de estos ataques, y la ciudadanía sufre permanentemente todo tipo fraudes, delitos y violaciones a su privacidad mediante operaciones por internet. Se ratifique o no el convenio, debemos tomar medidas concretas para fortalecer nuestra capacidad de enfrentar estos fenómenos delictivos y minimizar sus peores efectos. Son acciones que no pueden esperar." READ MORE

RELATED ARTICLES

Exhortación para que el estado mexicano se adhiera a las disposiciones del convenio sobre ciberdelincuencia del consejo de Europa y su protocolo adicional, 19 Aug 2020

Source: diarioextra.com

Date: 25 Aug 2020

Costa Rica: Las telecomunicaciones al servicio de la justicia

"Desde el punto de vista normativo, nuestro país cuenta con una valiosa herramienta para atacar los delitos informáticos, en el año 2017, la Asamblea Legislativa aprobó mediante Ley N° 9452, la adhesión al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001), que dota de instrumentos de cooperación internacional, creando una red permanente de contactos 24/7 con procedimientos para solicitar rápidamente información y documentación que puedan servir de pruebas para la investigación de delitos informáticos, permitiendo mejorar la eficiencia y la eficacia judicial de este tipo de delitos." READ MORE

Source: financialexpress.com

Date: 26 Aug 2020

Potential areas of Strategic Cooperation of India with Paraguay: Space Cooperation, Cybersecurity and Citizen Defense

"In 2017, through Law No. 5.994/17, Paraguay acceded to the Budapest Convention on Cybersecurity and its Additional Protocol, the main objective of which is to pursue a common criminal policy aimed at protecting society against cybercrime, especially through the adoption of appropriate legislation and the promotion of international cooperation. Currently, as a State party to this Convention, the country is a beneficiary of the GLACY+ (Global Action against Extended Cybercrime) programme, carried out by the Council of Europe together with the EU, in order to support member countries in order to achieve the effective implementation and harmonization of the Convention to national positive legislation, through the promotion of legislative strategies against cybercrime, capacity building of justice operators and international legal cooperation. […] The development of a strategic alliance between the Ministry of Information and Communication Technologies of Paraguay and the Ministry of Technological and Electronic Information together with the National Information Center of India would be a lead, to extensive cooperation for the benefit of our new institutions and finally to the training and capacity building of human resources in this area." READ MORE

Source: Bloomberg

Date: 26 Aug 2020

New Zealand Stock Trading Interrupted by Second Cyber Attack

"New Zealand's stock exchange was halted for more than three hours on Wednesday as it came under cyber attack for a second day. Exchange operator NZX halted its cash markets at approximately 11:24 a.m. in Wellington and trading didn't resume until 3 p.m. Today's issue was "similar" to yesterday's cyber attack that disrupted the final hour of trading, NZX said in a brief statement. The NZX website and feed of company announcements also went down, but have since been restored. "This is a very serious attack on critical infrastructure in New Zealand," said Dave Parry, a professor of computer science at Auckland University of Technology. "The fact that this has happened on a second day indicates a level of sophistication and determination which is relatively rare." Cyber attacks aren't common in New Zealand but in neighboring Australia there has been an increase in incidents." READ MORE

Source: moneylaundering.com

Date: 27 Aug 2020

After Brief Pause, North Korea Resumes Cyberthefts Against Global Banks and ATMs

"North Korean government-sponsored hackers are still draining millions of dollars from banks and ATMs across the world in a cybertheft campaign that benefits the country's leadership, a U.S. interagency group has found. In an 18-page advisory, the FBI, Treasury Department and two cybersecurity agencies claim that in February, "North Korea's intelligence apparatus" ordered a team of hackers—which U.S. officials have dubbed the "BeagleBoyz"—to resume attacking and stealing cash from ATMs worldwide as part of a strategy that began in earnest in 2015 before petering out late-last year." READ MORE

Source: The United States Department of Justice

Date: 27 Aug 2020

United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors

"The Justice Department today filed a civil forfeiture complaint detailing two hacks of virtual currency exchanges by North Korean actors. These actors stole millions of dollars' worth of cryptocurrency and ultimately laundered the funds through Chinese over-the-counter cryptocurrency traders. The complaint follows related criminal and civil actions announced in March 2020 pertaining to the theft of $250 million in cryptocurrency through other exchange hacks by North Korean actors. […] As alleged in the complaint, in July 2019, a virtual currency exchange was hacked by an actor tied to North Korea. The hacker allegedly stole over $272,000 worth of alternative cryptocurrencies and tokens […]. Over the subsequent months, the funds were laundered through several intermediary addresses and other virtual currency exchanges. In many instances, the actor converted the cryptocurrency into BTC, Tether, or other forms of cryptocurrency – a process known as "chain hopping" – in order to obfuscate the transaction path. As detailed in the pleadings, law enforcement was nonetheless able to trace the funds, despite the sophisticated laundering techniques used." READ MORE

Source: Cyberscoop

Date: 26 Aug 2020

Two accused email scammers from Ghana extradited to US to face fraud-related charge

"Two accused scammers have arrived in the U.S. from Ghana to face charges that they were involved in separate conspiracies to defraud American victims out of millions of dollars. Deborah Mensah, a 33-year-old Ghanaian national, stands accused of stealing more than $10 million through business email compromise (BEC) fraud, in which she allegedly targeted businesses and elderly individuals as part of an international scam. Mensah is the eighth person to be charged as part of the investigation, the U.S. Department of Justice said Wednesday. The department also announced that another accused BEC scammer, Maxwell Peter, had been extradited to the U.S. to face charges in an unrelated case." READ MORE

RELATED ARTICLES

US DoJ, Ghanaian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy, 26 Aug 2020

Source: TechWire Asia

Date: 19 Aug 2020

Phishing scams dominate the Philippines cybercrime landscape

"Cybercrime in the Philippines is on a rapid rise, with phishing campaigns alone up 200% since the country went into lockdown in March. In today's highly-digitalized society, wanton cybercrimes have proven to be difficult to eradicate, and the cyberattack threat matrix just got riskier when recent quarantine and lockdown restrictions forced everyone indoors. […] In the Philippines, the pandemic has brought out the worst in some opportunists, and in the virtual realm, it appears phishing attacks are the cyber weapon of choice. The Philippines has been trying to enforce legislation on engineered phishing scams for years now, but with so many Filipinos online all the time during the pandemic, the National Bureau of Investigation's Cybercrime Division recorded a 200% increase since the lockdowns started back in March. Phishing is being listed by Philippine authorities as the top cybercrime being committed in the country during the COVID-19 pandemic, followed by online selling scams and the spread of fake news." READ MORE

Source: The New York Times

Date: 25 Aug 2020

Facebook Plans Legal Action After Thailand Tells It to Mute Critics

"Facebook is planning legal action against the government of Thailand for ordering the social media platform to partially shut down access to a group critical of the Thai monarchy, the company said on Tuesday. On Monday, Facebook began preventing users in Thailand from accessing Royalist Marketplace, a Facebook group with more than a million members that was set up by a self-exiled Thai academic living in Japan. Thailand has some of the world's strictest lèse-majesté laws, which make it a crime to criticize members of the royal family. Other legislation, including a sedition law and a computer crimes act, have also been used to target critics of the royal family, even as protesters have taken to the streets in recent weeks to call for the monarchy's power to be curbed." READ MORE

Source: Human Rights Watch

Date: 28 Aug 2020

Belarus: Internet Disruptions, Online Censorship

"Belarusian authorities are disrupting internet access and restricting content online in response to peaceful, countrywide protests, Human Rights Watch said today. [...] The blocking appeared to be an attempt to silence information about protests and severe police brutality against their participants, Human Rights Watch said. [...] In 2015, United Nations and regional organization experts said: "Using communications 'kill switches' (i.e. shutting down entire parts of communications systems) can never be justified under human rights law." Governments also have an obligation to ensure that any restrictions to information online are provided by law, are a necessary and proportionate response to a specific threat, and are in the public interest. The UN General Assembly Resolution on "Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association" says that governments should refrain from shutting down the internet as well as from imposing content restrictions that violate the legality, necessity, and proportionality criteria. Prohibition of internet disruptions by governments in relation to peaceful assemblies was reiterated by General Comment Number 37 on the right of peaceful assembly by the UN Human Rights Committee, which interprets the International Covenant on Civil and Political Rights." READ MORE

Source: MIT Technology Review

Date: 25 Aug 2020

Israeli phone hacking company faces court fight over sales to Hong Kong

"Human rights advocates filed a new court petition against the Israeli phone hacking company Cellebrite, urging Israel's ministry of defense to halt the firm's exports to Hong Kong, where security forces have been using the technology in crackdowns against dissidents as China takes greater control. In July, police court filings revealed that Cellebrite's phone hacking technology has been used to break into 4,000 phones of Hong Kong citizens, including prominent pro-democracy politician and activist Joshua Wong. He subsequently launched an online petition to end Cellebrite's sales to Hong Kong, which gained 35,000 signatures. [...] Hong Kong's new security law, which increases Beijing's control of the city, defines pro-democracy protests as terrorism, severely limits free speech, and reduces much of the autonomy that the city once had from China. As of May, the United States no longer considered Hong Kong autonomous from the mainland." READ MORE

Source: convergenciadigital.com

Date: 24 Aug 2020

Brasil sofreu mais de 2,6 bilhões de ataques cibernéticos no 1º semestre

"O Brasil sofreu mais de 2,6 bilhões de tentativas de ataques cibernéticos de janeiro a junho, de um total de 15 bilhões em toda a América Latina e Caribe, revelou estudo Fortinet Threat Intelligence Insider Latin America [...]. No último trimestre, a empresa registrou um aumento considerável de ataques de "força bruta" na região, que são as tentativas repetidas e sistemáticas de adivinhar uma credencial enviando diferentes nomes de usuário e senhas para acessar um sistema." READ MORE

Source: cio-mag.com

Date: 20 Aug 2020

Le Cameroun au taquet contre la cybercriminalité

"Depuis la semaine dernière le Cameroun bat une importante campagne contre la cybercriminalité. Avec des pertes importantes causées par ce fléau, il est question de prévenir, de sensibiliser et de développer davantage de moyens de lutte. « La cybercriminalité est un phénomène qui n'épargne aucun Etat, aucune institution, aucun individu. Le Cameroun n'en est pas épargné et subit les conséquences désastreuses de ce fléau, tant sur les biens que sur les individus », a déclaré Minette Libom Li Likeng, la ministre des postes et des télécommunications [...]. D'après elle, le contexte qui prévaut actuellement au Cameroun est marqué par la montée en puissance de ce phénomène. Cela se traduit par l'incitation à la révolte contre les institutions de l'Etat, la diffusion sur les réseaux sociaux d'informations erronées et images montées de toutes pièces, pour désinformer, choquer, semer la psychose au sein de l'opinion, et jeter le discrédit sur le pays et le piratage des sites web et comptes Facebook de hautes personnalités et institutions." READ MORE

Latest reports

- New Zealand Government, Public consultation on a proposal for New Zealand to join the Budapest Convention on Cybercrime, July 2020
- Organization of American States, Cybersecurity Capacity Review of Brazil, 21 August 2020
- Banco Interamericano de Desarrollo, OAS, Centro Global de Capacidad en Seguridad Cibernética - Universidad de Oxford | REPORTE CIBERSEGURIDAD 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe
- Council of Europe, Achievements of the grantees of the Council of Europe project EndOCSEA@Europe, 31 August 2020
- EU Cyber Direct: Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU Cooperation, 25 August 2020
- United Nations Interregional Crime and Justice Research Institute (UNICRI), Towards Responsible Artificial Intelligence Innovation, 2020
- Anti-Phishing Working Group (APWG), Phishing Activity Trends Report 2nd Quarter 2020, 27 August 2020
- Maillart, J. Les limites de la territorialité objective face à la cybercriminalité, 27 August 2020
- Statescoop, Ransomware attacks map, updated in August 2020
- ICANN: Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, July 2020

Upcoming events

- 31 August–2 September, Armenia (online) – Development of Standard operating procedures for Cooperation between CSIRT and Law Enforcement for Armenia, CyberEast
- 1-15 September, Albania (desk review) – Desk assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- 1-15 September, Bosnia and Herzegovina (desk review) – Desk assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- 1-15 September, Montenegro (desk review) – Desk assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- 1 September–15 October, Namibia – Support for drafting the Data Protection Law, in collaboration with the Data Protection Unit of the Council of Europe, GLACY+
- 3 September, Jordan (online) – First national on the development of a domestic Standard Operating Procedures and toolkit for first responder/cybercrime investigation and e-evidence in Jordan, CyberSouth
- 4 September 2020, Georgia (online) – Technical webinar: preparation for elections security, CyberEast
- 9-11 September, Georgia (online) – Development of Standard operating procedures for Cooperation between CSIRT and Law Enforcement for Georgia, CyberEast
- 10-11 September, Strasbourg (online) – Second HELP Working Group Meeting for the development of a HELP Course on Cybercrime
- 14-16 September, Moldova (online) – Development of Standard operating procedures for Cooperation between CSIRT and Law Enforcement for Moldova, CyberEast
- 14-18 September, Brussels (online) – EU Cyber Forum, GLACY+, iPROCEEDS-2, CyberEast, CyberSouth
- 14-30 September, online – E-First Course, in collaboration with ECTEG and INTERPOL, GLACY+
- 15 September, Georgia (online) – Table-Top Exercise for Policy Makers: Preparation and coordination for election security, CyberEast
- By 15 September, C-PROC – Finalisation of studies on judicial training systems and capabilities and on international cooperation, CyberSouth
- By 15 September, C-PROC – Review of the Introductory Judicial Course on Cybercrime and Electronic Evidence, 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 August 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