Cybercrime Digest

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

16-30 June 2020

Source: Council of Europe

Date: 30 Jun 2020

C-PROC series of cybercrime webinars continue: materials available, next topics and dates announced

Initiated in April, the C-PROC series of webinars on cybercrime have continued in the second half of June with more sessions, respectively dedicated to *Cybercrime in Africa and the challenges of international cooperation*, co-organized by the U.S. Departement of Justice (USDoJ) and the Council of Europe in the framework of the GLACY+ Project, *Introduction to Cyberviolence*, conducted in the framework of the CyberEast Project, *Cybercrime and Criminal Justice in Cyberspace* the regional seminar dedicated to Asisa-Pacific, under the GLACY+ Project, and *International standards on collection and handling of electronic evidence*, under the CyberSouth Project.

New webinars are scheduled for the next period: *Cybercrime and Criminal Justice in Cyberspace*, the series of seminars hosted by the European Union and the Council of Europe (Africa, EN - 7 July 2020; Africa, FR - 9 July 2020; Latin America and Caribbean, EN - 20 July; Latin America and Caribbean, ES - 22 July]. For further updates, please check our webinars dedicated webpage.

Source: Council of Europe

Date: 1 Jul 2020

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

"CyberSouth project organised a regional online workshop on interagency cooperation on the search, seizure and confiscation of on-line crime proceeds, on the 1st of July 2020. The event gathered around 30 participants from Law Enforcement agencies, Financial Investigation Units and prosecutors of priority countries as well as experts from United Kingdom, Romania and FBI. The aim of the workshop was to assist authorities of the project countries to increase their knowledge on fighting against cybercrime and targeting on-line crime proceeds." READ MORE

Source: Europol

Date: 19 Jun 2020

Exploiting isolation: sexual predators increasingly targeting children during COVID pandemic

"Video calls with friends and family, social media interaction, online games, educational use: during the corona lockdown children's lives promptly shifted even further from the real world into an online virtual one. Sex offenders have found in this development a tempting opportunity to access a broader group of potential victims. The report published today by Europol shines a light on the increased sharing of child sexual exploitation images online and how to confront this serious threat to children's safety. To confront this threat, law enforcement has also increased its efforts to tackle this severe crime, which sees a child being re-victimised every time an image is shared. […] Europol is monitoring the threat and providing continuous support to Member States to identify offenders and victims. With its "Trace an object" campaign, Europol has involved the public in providing leads for the identification of victims and offenders. The Europe wide #SayNo campaign brings awareness to children on the dangers they face sharing explicit material online." READ MORE

Source: Reuters

Date: 29 Jun 2020

Germany uncovers massive online child abuse network

"German cyber crime authorities have uncovered a massive online network of at least 30,000 people who share child pornography and exchange advice on how to sedate and abuse minors […]. Peter Biesenbach, justice minister in the western state of North Rhine-Westphalia, said investigators were stunned by the scale of the network and that a special task-force has been set up to find the suspects and bring them to justice. People log on to a chat, not on the dark web, but on messenger services on the normal web," said Biesenbach. "They get instructions from other users on what sedatives one should give children in order to abuse them." READ MORE

Source: Enisa

Date: 26 Jun 2020

The EU Cybersecurity Act's first anniversary: one step closer to a cyber secure Europe

"On 27 June 2020, the European Union Agency for Cybersecurity (ENISA) celebrates the first anniversary of the EU Cybersecurity Act (CSA) and its strengthened role towards securing Europe's information society. The CSA gave the Agency a permanent mandate, a new list of tasks and increased resources, and also established the EU cybersecurity certification framework. The Agency now plays a key role in setting up the framework and builds on its past work towards achieving a high common level of cybersecurity across the European Union by actively supporting Member States, EU institutions, industry, academia and citizens. Regarding the framework, the Agency is close to completing the first cybersecurity certification scheme and is making rapid progress towards a second one, on cloud services." READ MORE

Source: Israel Defense

Date: 18 Jun 2020

INTERPOL Cybercrime Director: Global Coordinate Response Needed to Combat Cybercrime

"Some 50 percent of crime is now being committed online and as such law enforcement around the world must adapt its modus operandi to protect communities, Craig Jones, director of Cybercrime at International Criminal Police Organization (INTERPOL) said […]. "Our mandate is to reduce the global impact of cybercrime and protect communities for a safer world," he said. To accomplish this task, he said a "global coordinated response" is needed - one that has to "deliver both preventive measures and operational activities." To that effect INTERPOL has designed three main pillars: Cybercrime threat response, cybercrime operations and cybercrime capabilities development. Jones said that first and foremost, law enforcement needs to "develop a better understanding of the cybercrime landscape." READ MORE

Source: ZD Net

Date: 22 June 2020

BlueLeaks: Data from 200 US police departments & fusion centers published online

"An activist group has published on Friday 296 GB of data they claim have been stolen from US law enforcement agencies and fusion centers. The files, dubbed BlueLeaks, have been published by Distributed Denial of Secrets (DDoSecrets), a group that describes itself as a "transparency collective". […] According to DDoSecrets, most of the files are police and FBI reports, security bulletins, law enforcement guides, and more. Some of the files also supposedly contain sensitive and personal information, such as names, bank account numbers, and phone numbers." READ MORE

Source: Channel News Asia

Date: 26 June 2020

Singapore: Cybercrime jumps more than 50% in 2019, new threats emerge from COVID-19 pandemic

"Cybercrime cases jumped by more than 50 per cent last year, accounting for more than a quarter of all crimes committed in the country, said the Cyber Security Agency of Singapore (CSA) in its annual report published on Friday (Jun 26). There were 9,430 cybercrime cases reported last year, up 51.7 per cent from the 6,215 cases reported in 2018, according to the key findings from the Singapore Cyber Landscape 2019 report. The common types of cybercrime were e-commerce scams, phishing and malware attacks. The CSA, an agency managed by the Ministry of Communications and Information, said its data revealed how threats and attacks have grown in both "scale and complexity". The COVID-19 pandemic has also created a new raft of vulnerabilities, with attackers exploiting the panic and fear to seek financial gain or gain access to classified information." READ MORE

Source: Listin Diario

Date: 26 Jun 2020

Republica Dominicana, la ciberdelincuencia aumentó un 235 % durante los meses de la pandemia

"De acuerdo a informaciones suministradas por el Centro Nacional de Ciberseguridad (CNCS), los ciberdelincuentes aprovecharon que los usuarios están más conectados en la rede para aumentar el miedo y la desinformación en esta pandemia. De acuerdo a las estadísticas del CNCS, el país registró un incremento del 235%, entre marzo y mayo, en comparación con ese mismo periodo de 2019. En concreto, en esos meses de pandemia se registraron 1,211,000 eventos botnet en comparación con los 361,000 del año pasado", explicaron. […] Durante la pandemia, el ataque de phishing es el vector más efectivo para los ciberatacantes debido al aumento de los usuarios que trabajan de manera remota y, en muchos casos, lo hacen fuera de la seguridad con la que cuentan a lo interno de la organización." READ MORE

Source: World Economic Forum

Date: 29 Jun 2020

Three ways governments can address cybersecurity in the post-pandemic world

"The increased adoption of telework and distance learning due to "social distancing" have led to a 50% increase in data traffic in some markets. […] Despite the current challenges, the cyber community can work together to guarantee security, privacy and digital rights. To seize the opportunity, governments must take three specific actions.

1. Adjust national frameworks: countries must become more agile in updating or developing national cybersecurity strategies, as well as legal and regulatory framework regarding cyberspace. […] Harmonizing legislation should also be a priority. Today, the Budapest Convention is the most global and inclusive agreement dedicated to fighting cybercrime. It has been ratified by 65 countries, with another 11 invited to accede. The Organization of American States recommends adhesion to the Convention, and international organizations and countries should consider it a means to achieve immediate international cooperation on information sharing and cross-border investigation.

2. Increase international cooperation: cybersecurity requires international cooperation, and there is a need to increase trust, at all levels, between countries and industries. […]

3. Unify awareness campaigns: no one is immune to a cyber incident or one "bad click." We must increase awareness at all ages and levels, regardless of industry. In particular, it is of utmost importance to start teaching children about cybersecurity." READ MORE

Source: GCN

Date: 22 Jun 2020

U.S., lawmakers combat flood of COVID cyber fraud

"Nearly 50 million Americans have filed COVID-19-related complaints with the Federal Trade Commission, and the number of daily complaints to the FBI's Internet Crime Complaint Center has more than tripled over the past four months, according to FBI Deputy Assistant Director Tonya Ugoretz. […] Lawmakers have put forward a number of bills designed to address cyber fraud during and after the pandemic: (i) The Internet Fraud Prevention Act would require the FBI, Federal Trade Commission and Federal Reserve to study and report on business email compromise; (ii) The COVID-19 Restitution Assistance Fund for Victims of Securities Violation Act would provide individuals up to $50,000 in restitution if they are victims of securities fraud related to the coronavirus; (iii) The Senior Investor Pandemic Fraud Protection Act would create a new grant program for states to protect senior citizens and other vulnerable adults from COVID-related fraud; (iv) The S. Secret Service Mission Improvement and Realignment Act would move the U.S. Secret Service -- which investigates financial crimes -- back to the Department of Treasury, to better combat cybercrime and counterfeit currency." READ MORE

Source: Dark Reading

Date: 23 Jun 2020

Cybercrime infrastructure never really dies

"Despite the takedown of the "CyberBunker" threat operators in 2019, command-and-control traffic continues to report back to the defunct network address space. […] The CyberBunker operated in Germany is the second such facility raided by police. In 2013, the first CyberBunker — based in Amsterdam and operated by some of the same people — was shut down by police, following extended distributed denial-of-service attacks against anti-spam coalition SpamHaus. […] Nine months after German police raided a Cold War-era bunker and shut down the group operating the cybercriminal service, command-and-control (C2) traffic and other network data continue to attempt to use the Internet address space assigned to the group, according to an analysis published by the SANS Technology Institute on Tuesday." READ MORE

Source: The Chronicle

Date: 20 Jun 2020

The Gambia: Cyber Security in the Third Republic

"The global village that we live in today enables the billions of its inhabitants to communicate daily thanks to various devices. […] However, the world wide web (www.) sometimes serves as a safe haven for various criminals operating under the radar since legislation for this arena has not been developed to its full potential to counter the cybercriminals emerging daily around the globe. On June 16th, 2020, the U.S Department of State and the Council of Europe hosted a webinar on: "Challenges of International Cooperation on Cybercrime and Electronic Evidence in the Africa Region" according to the Council of Europe. […] The Budapest Convention on Cybercrime was at the core of the training program organized in an effort to encourage its implementation by all member States as well as the recruitment of new nations to join the cause. […] In December 2019, the Ministries of Justice and the one of Information and Communication of The Gambia prepared a draft Cybercrime Bill which was finalized in December 2019 and open for public consultation until January 2020. […] In The Gambia, every day that goes by, many victims on the commonly utilized social media platforms are approached by cyber criminals. […] These professionals operate from remote areas of the world as well as on the Gambian territory and utilize state of the art techniques that enable them to re -route their communications across a network of global servers. Their IP addresses change by the second […] and make it hard for the authorities to stay on their tracks." READ MORE

Source: Milenio

Date: 17 Jun 2020

México: Fundamental proteger datos personales en la era digital

"El Sistema Nacional de Transparencia pidió a los estados proteger los datos personales y el derecho al acceso a internet porque han identificado conductas de abuso e indebido tratamiento de la información personal en el ámbito digital que genera violencia digital y graves daños a niños y mujeres, fundamentalmente. El comisionado mexiquense, Gustavo Parra Noriega, autor de la propuesta avalada a nivel nacional, advirtió que es urgente dar garantías a los usuarios y que ellos a su vez establezcan las mayores medidas de seguridad de su información para que no sea usada en actividades ilícitas o que afecten su moral." READ MORE

Source: Senado, Paraguay

Date: 29 Jun 2020

Paraguay: CONAREP debatió sobre procedimientos para obtención de datos informáticos

"La Comisión Nacional para el Estudio de la Reforma del Sistema Penal y Penitenciario (CONAREP) […] se reunió en forma presencial. En la fecha, se prosiguió con el análisis de la parte Procesal Penal, relativo a los procedimientos para la obtención de datos informáticos. En ese sentido, la diputada Rocío Vallejo, explicó que han consensuado algunos artículos y otros que requieren de más ajustes, ya que, "se establece, por ejemplo, el allanamiento remoto de datos y también hemos convenido en que se va buscar la mejor redacción para el artículo 200 (Intervención de comunicaciones)", expresó. Señaló la legisladora que, con relación a este punto, sobre la interceptación de comunicaciones, deben analizarlo en forma general y teniendo en cuenta toda la tecnología que está surgiendo, debido a que, el Código Procesal Penal, ya tiene 22 años. En ese sentido, indicó que, "es mucha la tecnología que fue surgiendo y debemos adecuarnos al Convenio de Budapest y las observaciones que nos hicieron los consultores internacionales, en este tema". READ MORE

Source: The News

Date: 20 Jun 2020

Pakistan: Efforts afoot to amend cybercrime law

"Pakistan Commission for Human Rights (PCHR) in collaboration with UNESCO and Parliamentary Task force on Sustainable Development Goals (SDGs) has prepared a set of amendments to Prevention of Electronic Crime Act 2016 and suggested removal of a legal clause dealing with PTA's power to remove or block information in the interest of the glory of Islam or the integrity, security and defense of Pakistan, decency or morality. […] However, the document added, it is important to repeat that in principle a section dealing with censorship of online content does not sit with the preamble or scheme of a Cybercrime Act as this has nothing to do with curbing cybercrime and does not carry any civil or criminal liability." READ MORE

Source: Fiji Sun

Date: 27 Jun 2020

UniFiji Urges Standing Committee To Consider Hate Crimes And Cyberterrorism In Legislation

"The Submissions from the University of Fiji School of Law requested the Parliamentary Standing Committee to consider the Siracusa Principles when discussing the Cybercrime Bill 2020, especially in relation to section 17 (2) of the Bill which may be ambiguous in relation to constitutional rights protection in Fiji. In addition, the University of Fiji submissions urged the Standing Committee members to consider including both hate crimes and cyberterrorism as additional clauses in the proposed legislation." READ MORE

Source: APWG.EU

Date: 1 Jul 2020

LOCARD Webinar on Electronic Evidence on 16 July

"In their fight against cybercrime, one of the most difficult challenges for several countries is to standardise the process used in the preparation and generation of digital forensic reports. The procedure needed to obtain digital evidence, as well as its recognition in a court of justice, should follow standardised procedures aimed at guaranteeing the origin of the evidence and the integrity of the chain of custody. This is a crucial step towards producing high quality reports and a way to encourage digital forensics best practices and facilitate sharing and admissibility of reports across jurisdictions. REGISTER NOW in the two-part webinar that will take place next 16th July 2020 aimed at addressing these and other related needs." READ MORE

Latest reports

- Council of Europe, Cybercrime and COVID19 webpage, updated weekly
- Cross-border Data Forum, Budapest Convention: what is it and how is it being updated?, 2 July 2020
- Europol, European Union Terrorism Situation and Trend report (TE-SAT), 23 June 2020
- European Commission, Victims' Rights: New Strategy to empower victims, 24 June 2020
- ICANN, ICANN68 GAC Communiqué – Virtual Policy Forum, 27 June 2020
- Leyes, Perú, Proyecto de ley de seguridad informática y represión de los delitos informáticos, 25 June 2020
- ASPI, Covid-19 Disinformation & Social Media Manipulation, 25 June 2020
- APWG, Phishing Activity Trends Reports: 1st Quarter Report 2020
- Ministerio Publico Portugal, New Law on Computer Crime in Macau, May 2020

Upcoming events

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 June have been rescheduled to a later date.

- 1 July, Seminar on the Budapest Convention in the framework of the e-Evidence Bootcamp online course, INTERPOL, GLACY+
- 1 July Online regional event on interagency cooperation between cybercrime units, financial investigators, financial intelligence units and prosecutors in the search, seizure and confiscation of online crime proceeds, CyberSouth
- 3 July, Webinar on International standards on collection and handling of electronic evidence, CyberSouth
- 5 July, Report on Cybercrime in Africa (First African Forum), GLACY+
- 6 July, Review of Cybercrime Legislation of Liberia, GLACY+
- 7 July, EU-CoE joint Webinar on Criminal justice and cybercrime in cyberspace for the African Region (EN), GLACY+
- 9 July, EU-CoE joint Webinar on Criminal justice and cybercrime in cyberspace for the African Region (FR), GLACY+
- 15-17 July, Online workshop on Data Protection and INTERPOL tools, GLACY+

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