Cybercrime Digest

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

1-15 June 2019

Source: European Commission

Date: 6 Jun 2019

Security Union, Commission receives mandate to start negotiating international rules for obtaining electronic evidence

"Today, EU Member States agreed to give two mandates to the Commission to engage in international negotiations to improve cross-border access to electronic evidence in criminal investigations. The Council agreed to provide the Commission with negotiating mandates for negotiations with the United States and for the Second Additional Protocol to the Council of Europe "Budapest" Convention on Cybercrime. Both mandates include provisions on strong fundamental rights safeguards on data protection, privacy and the procedural rights of individuals, which will have to be an integral part of any future agreement. […] With the majority of criminal investigations requiring access to evidence based online and often outside the EU, it is crucial to ensure an effective cooperation and compatible rules at international level. […] The mandates require strong and specific safeguards on data protection, privacy and the procedural rights of individuals based on fundamental rights, freedoms and general principles of EU law in the Treaties and Charter of Fundamental Rights." READ MORE

Source: Fratmat Info

Date: 13 Jun 2019

Cybercriminalité: La Côte d'Ivoire adhère à la convention de Budapest

"Dans le cadre de la lutte contre la cybercriminalité, la Côte d'Ivoire a décidé d'adhérer à la convention de Budapest. L'annonce a été faite le mercredi 12 juin 2019, par le porte-parole du gouvernement, Sidi Touré. « L'adhésion de la Côte d'Ivoire à la Convention de Budapest témoigne de sa forte implication dans la lutte contre la cybercriminalité et de son attachement à la coopération internationale en matière de cybersécurité », a expliqué le ministre Sidi Touré, à l'issue du Conseil des ministres. A en croire l'émissaire du gouvernement ivoirien, cette Convention est un instrument juridique visant à harmoniser les législations nationales pénales tout en fournissant les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions commises au moyen d'un système informatique." READ MORE

Source: Eurojust

Date: 7 Jun 2019

Tackling cybercrime through joint investigation teams

"Joint investigation teams are one of the most effective tools for investigators confronted with the challenge of fighting cybercrime. Due to the fast-paced, cross-border nature of cybercrime, judicial and police authorities face specific challenges, such as the need to act quickly, overcome the differences in legislation between countries concerning how to collect and secure e-evidence, ensure swift cooperation with third countries and actors in the private sector, and ensure data security. On 5-6 June, experts on joint investigation teams from national authorities and EU institutions met at Eurojust to explore how to effectively deal with these obstacles in cybercrime investigations and maximise the potential of joint investigation teams to address this growing security concern." READ MORE

Source: ZD Net

Date: 7 Jun 2019

For two hours, a large chunk of European mobile traffic was rerouted through China

"For more than two hours on Thursday, June 6, a large chunk of European mobile traffic was rerouted through the infrastructure of China Telecom, China's third-largest telco and internet service provider (ISP). The incident occurred because of a BGP route leak at Swiss data center colocation company Safe Host, which accidentally leaked over 70,000 routes from its internal routing table to the Chinese ISP. The Border Gateway Protocol (BGP), which is used to reroute traffic at the ISP level, has been known to be problematic to work with, and BGP leaks happen all the time. However, there are safeguards and safety procedures that providers usually set up to prevent BGP route leaks from influencing each other's networks. But instead of ignoring the BGP leak, China Telecom re-announced Safe Host's routes as its own, and by doing so, interposed itself as one of the shortest ways to reach Safe Host's network and other nearby European telcos and ISPs." READ MORE

Source: Sarahpepen

Date: 12 Jun 2019

Celebran Conferencia Regional sobre Políticas y Estrategias contra la Ciberdelincuencia

"El Consejo de Europa, a través del Proyecto Acción Global contra la Ciberdelincuencia Extendido (GLACY+), cofinanciado por la Unión Europea, organizó, con el apoyo del Gobierno Dominicano y la Agencia de Implementación de Crimen y Seguridad de CARICOM (CARICOM IMPACS), la conferencia regional para los países de la Comunidad del Caribe, orientada a facilitar el desarrollo de políticas y estrategias específicas contra la ciberdelincuencia. Esta conferencia está compuesta por funcionarios involucrados en el desarrollo y reforma de políticas nacionales, estrategias y legislación en materia de tecnologías de la información en 28 países de la region del Caribe como es Antigua y Barbuda, Anguila, Aruba, Bahamas, Barbados, Belice, Bermuda, Cuba, Curazao, Colombia, Dominica, Granada, Guyana, Haití, Islas Caimán, Islas Turcas y Caicos, Islas Vírgenes Británicas, Jamaica, México, Montserrat, Puerto Rico, Saint Kitts y Nevis, San Vicente y las Granadinas, Santa Lucía, Saint Martin, Surinam, Trinidad y Tobago y República Dominicana." READ MORE

Source: Daily Mirror

Date: 15 Jun 2019

Sri Lanka, Data Protection Law in two months

"Data Protection Bill which provides measures to protect an individual's personal data held by banks, telecom companies, hospitals and other institutions will be presented to Parliament in two months time, Non-Cabinet Minister of Digital Infrastructure and Information Technology, Ajith P. Perera said yesterday. He told a news conference that using data pertaining to individuals for wrongful purposes will be restricted under this law. "The new legislation will impose restrictions on banks, telecom companies and even hospitals using data for any purpose without the consent of the individual concerned," the non-Cabinet minister said. He said the new legislation will not restrict the right of the people to obtain information guaranteed under the Right to Information Act. "Data Protection law will actually make the Right to Information Act more effective," the Non-Cabinet minister said. He said the new legislation is still in the drafting stage and that the People's views on the new legislation will be called for on July 27, at Cinnamon Grand Hotel." READ MORE

Source: Jamil Chade

Date: 9 Jun 2019

Brasil não está preparado para combater globalização do crime

"O Brasil precisa de uma lei geral de cooperação internacional para combater o crime e a corrupção e, apesar dos avanços na Operação Lava Jato, o país continua "muito atrasado nesse campo". O alerta é de Vladimir Aras, candidato ao cargo de Procurador-Geral da República e ex-secretário de Cooperação Internacional do MPF entre 2013 e 2017. Em entrevista ao blog, Aras traçou os avanços registrados nos últimos anos e destacou as dificuldades ainda existentes no país. A eleição ocorre no dia 18 de junho. Pare ele, o Brasil "infelizmente não está preparados para dar conta desse problema, porque não temos polícia de fronteiras; porque, salvo pelo excelente serviço prestado pela Marinha do Brasil, não temos embarcações suficientes para a guarda costeira; porque não usamos adequadamente as tecnologias disponíveis para fiscalização aduaneira, portuária e aeroportuária; e porque grandes extensões de nossas fronteiras não são devidamente fiscalizadas por falta de recursos públicos". "Por outro lado, ainda não implementamos todos as convenções internacionais a que nos obrigamos na luta contra o crime", disse. "Não somos partes em tratados importantes, como os do Conselho da Europa, a exemplo da Convenção de Budapeste, sobre cibercrime e de outras sobre transferência de condenados e extradição. Não temos sequer uma lei brasileira de cooperação internacional", alertou." READ MORE

Source: PUNCH

Date: 12 Jun 2019

Nigeria, Federal Government committed to cybercrime Act amendment

"The Head, Cybercrime Prosecution Unit, Federal Ministry of Justice, Terlumun Tyendezwa, says the Federal Government is committed to the amendment of the Cybercrime Act, 2015. Tyendezwa, who stated this at a media interactive session on the 'Constitutionality and Legality of the Cybercrime Act in Nigeria,' noted that the Act was not perfect. At the event organised by the Socio-Economic Rights and Accountability Project, in collaboration with the National Endowment for Democracy, United States, Tyendezwa said the Ministry of Justice was open to all stakeholders who would engage them on how the Act could be amended. He said, "From the point of the passage, we as the operators knew that there were things that needed to change. We are presently collating memoranda on the amendment of the Act. But an amendment takes time and costs money. "The Office of the Attorney General of the Federation and Ministry of Justice continues to place a high value on entrenching fundamental human rights and engaging with all stakeholders on the Cybercrime Act is one of our approaches."" READ MORE

Source: TechZim

Date: 4 Jun 2019

Zimbabwe, $42 Million Lost In The First Quarter Of 2019 Due To Cybercrime

"According to stats produced by the Zimbabwe Republic Police, over $40 million has been lost to cybercrime in the first quarter of 2019 alone. That's quite the number and presents a huge challenge to customers who don't seem to be getting as much protection from banks or the police force. Officials working on cybercrimes only managed to recover $1.468 million, down from last year's $1.68 million during the same period. This statistic is particularly alarming because it means only less than 4% of the money lost was recovered." READ MORE

Source: IT Web Africa

Date: 4 Jun 2019

Kenya: government websites attacked

"A group calling itself KURD Electronic Team have hacked 18 government websites in Kenya, bringing to question the East African country's official cyber readiness. Websites affected included the Integrated Financial Management System (IFMIS), National Youth Service, National Environment Trust Fund, Department of Petroleum, the Department of Planning, the National Development Implementation Technical Committee, Refugees Affairs Secretariat at Immigration, Kenya Meat Commission and the Lake Basin Development Authority. The Communication Authority (CA) issued a statement explaining the the sites had only been defaced and not hacked as alleged." READ MORE

Source: New York Times

Date: 15 Jun 2019

U.S. Escalates Online Attacks on Russia's Power Grid

"In interviews over the past three months, the officials described the previously unreported deployment of American computer code inside Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections. Advocates of the more aggressive strategy said it was long overdue, after years of public warnings from Homeland Security and the F.B.I. that Russia has inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States. But it also carries significant risk of escalating the daily digital Cold War between Washington and Moscow." READ MORE

Source: HackRead

Date: 13 Jun 2019

Telegram messaging service hit by massive DDoS attack

"The popular privacy-focused instant messaging application service Telegram has suffered a massive DDoS attack in which its service in the United States and several other countries has been disrupted, the company has revealed. The DDoS attack began targeting Telegram's servers around 12:20 PM – Jun 12, 2019. The company then sent out a series of tweets revealing the cause of service disruption. One such tweet stated that: "We're currently experiencing a powerful DDoS attack, Telegram users in the Americas and some users from other countries may experience connection issues." […] In Telegram's case, it is unclear why the service was targeted and who was behind the attack. However, speculations on Twitter are that the DDoS attack on the messenger service was launched due to its use by tens of thousands of activists protesting against Hong Kong's extradition law." READ MORE

Source: DW

Date: 6 Jun 2019

Germany: Dozens of raids over online hate speech

"Police have said they carried out searches in 13 federal states over crimes like incitement and the use of banned symbols. Authorities have struggled to enforce Germany's strict hate speech laws on social media. Police in Germany launched dozens of raids across the country on Thursday as part of a crackdown on incitement crimes being spread on the internet. The Federal Criminal Police Office (BKA) has said it searched residences in 13 federal states as part of a coordinated operation. […] Germany has been struggling to enforce its strict hate speech laws when it comes to comments made online, but the lack of concern most social media platforms have exhibited towards reining in racist and hateful content has left authorities and politicians searching for ways to get hateful speech offline." READ MORE

Source: The Conversation

Date: 13 Jun 2019

Actions Australia's government can take right now to target online racism

"Our government should extend Australia's participation in the European cybercrime convention by adopting the First Additional Protocol. In 2001 the Council of Europe opened the Budapest Convention on Cybercrime to signatories, establishing the first international instrument to address crimes committed over the internet. The add-on First Additional Protocol on criminalisation of acts of a racist and xenophobic nature came into effect in 2002. Australia's government – Labor at the time – initially considered including the First Additional Protocol in cyber crime legislation in 2009, and then withdrew it soon after. Without it, our country is limited in the way we collaborate with other country signatories in tracking down cross border cyber racism." READ MORE

Source: PR Newswire

Date: 14 Jun 2019

New EU initiative to counter surging wildlife cybercrime

"A new European Union-funded project aims to disrupt criminals trafficking wildlife in or via the EU using the internet, postal or fast parcel services. The project is implemented by a strong coalition gathering WWF, IFAW, INTERPOL, the Belgian Customs and TRAFFIC. The project is led by WWF Belgium, in affiliation with TRAFFIC. Funded by the Internal Security Fund of the Directorate General for Migration and Home Affairs of the European Commission, the two-year "Disrupting and dismantling wildlife cybercriminals and their networks in the European Union" project will help train customs, police and other enforcement officers across the EU to detect and deter wildlife trafficking. The project will also engage with delivery and online technology companies, to ensure wildlife traffickers do not exploit their services. […] Illicit trade in wildlife is estimated to be worth between 5-23 billion USD per year, making it one of the largest illegal global trade, after other transnational crimes such as drug trafficking and illegal logging, according to a 2017 Global Financial Integrity report." READ MORE

Latest reports

- Council of Europe, 21st T-CY Plenary – Draft Agenda, 8 Jul 2019
- Council of Europe, 4th Protocol Drafting Plenary – Draft Agenda, 9-11 Jul 2019
- European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Report on the implementation of the Action Plan Against Disinformation, 15 Jun 2019
- World Economic Forum, 5 futuristic ways to fight cyber attacks, 5 Jun 2019

Upcoming events

- 16-20 June, Algiers, Algeria – Adaptation of Judicial Training materials, CyberSouth
- 17-21 June, Tunis, Tunisia – OSINT training, CyberSouth
- 18-19 June, Bucharest, Romania – Participation in the launching event of the HELP online course on Data Protection, GLACY+
- 24-28 June, Tunis, Tunisia – Malware Analysis Training, CyberSouth
- 24-27 June, Marrakech, Morocco – Participation in the ICANN 65 - Policy Meeting, GLACY+
- 24-27 June, Accra, Ghana – International Data Protection Conference for the African Region, GLACY+
- 25-26 June, Santiago, Chile – Meeting of the Ibero American Network of Cyber Prosecutors (Cyber Red), GLACY+
- 25-27 June, INTERPOL, Singapore – Workshop on channels and avenues for international cooperation in cybercrime, GLACY+ / iPROCEEDS
- 26-27 June, Bucharest, Romania – Fourth annual Symposium on Cybersecurity Awareness organised by the Anti-Phishing Working Group (APWG), iPROCEEDS

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime