Cybercrime Digest

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

1-15 July 2018

Source: Council of Europe

Date: 13 Jul 2018

Evidence in cyberspace, WHOIS data, cyberviolence, global state of legislation in focus at the Octopus Conference

"The Octopus Conference 2018 focused on solutions to strengthen the rule of law in cyberspace through a Protocol to the Budapest Convention. Consultations with civil society, data protection experts and industry to review proposals for more effective ways to secure electronic evidence, in view of finalising the Protocol by the end of 2019, access to WHOIS data, cyber violence, the global state of cybercrime legislation and progress made through capacity building programmes were discussed by over 350 participants from all over the world." READ MORE

Source: Council of Europe

Date: 12 Jul 2018

Towards a Protocol to the Budapest Convention: Further consultations

"Following consultations with data protection, civil society, industry and others during the Octopus Conference on 12 July 2018, additional contributions are now sought. Stakeholders are invited to send written comments by 15 September 2018 on the provisional draft text on "emergency mutual assistance" and "languages of requests". Save the date: Further consultations on the Protocol are scheduled for Monday, 26 November, 14h00 – 18h00 at the Council of Europe in Strasbourg." READ MORE

RELATED ARTICLES

Council of Europe, Provisional draft text of provisions: Language of requests; Emergency MLA, 12 Jul 2018

Source: Samoa Observer

Date: 3 Jul 2018

Samoa combats cyber-crime

"Samoa took a step towards combating cyber-crime with the opening of the Council of Europe Cybercrime training yesterday. The two-day training event is supported by the Council of Europe and Australia's Department of Justice and Attorney General. The event was officially opened by Prime Minister Tuilaepa Dr. Sa'ilele Malielegaoi who welcomed presenters from Europe and Australia and expressed relief that assistance in terms of capacity building is now being offered. "This issue of cybercrime is not a matter that will affect Samoa in some distant time in the future, it is affecting Samoa right now," he said. "We have had illegal skimming of our cash flow machines and are affecting the day to day lives of our community today. In light of that, our guests have travelled here to assist us in building our national capacity as a nation so that we are more aware and better equipped to deal with such crimes." To ensure Samoa is on the same page with the international community in tackling cybercrime, the Prime Minister confirmed his Government's plans to ratify the Budapest Convention." READ MORE

RELATED ARTICLES

Samoa Planet, Samoa prepares to ratify the Budapest Convention, 4 Jul 2018

Source: The Telegraph

Date: 3 Jul 2018

Online child abuse investigations blocked by EU data crackdown, National Crime Agency warns

"Investigations into online child abuse risk being "significantly hampered" by the recent EU data crackdown, the National Crime Agency has warned. The agency said online criminals would be able to hide their identity because new data protection laws affect a vital database of website owners used to fight cybercrime. The "Whois" registry contains names and contact details for millions of website owners but police forces have seen access to the service throttled in recent weeks, making it harder to track down the owners of illegal websites. […] More than a month since the new law, Icann, the Los Angeles-based organisation that governs the system, has failed to reach an agreement with EU data regulators that would allow cybercrime units special access to the data. "Access to all current Whois data is vital for National Crime Agency and wider law enforcement investigations," NCA said. […] Several companies that offer access to the database have restricted the information across Europe in recent weeks, and some internet companies have allowed individuals to register new website names without having to provide their personal data." READ MORE

Source: The Telegraph

Date: 13 Jul 2018

Twelve Russian intelligence officers charged over US election hacking

"Twelve senior Russian intelligence officers have been charged with hacking into Democrat computers in a bid to sabotage the 2016 US presidential election. […] The Russians were accused of hacking into the computer networks of the Democratic National Committee and the presidential campaign of Hillary Clinton, targeting key email accounts, and then releasing the information on the internet. […] The Russians all belonged to the GRU, Russia's military intelligence agency. […] The Justice Department said the GRU in "official capacities engaged in a sustained effort to hack into the computer networks". They then released the hacked emails on the internet under the guises of DCLeaks and Gufficer 2.0. Mr Rosenstein said they used the cryptocurrency bitcoin to cover their tracks. It was not alleged that any vote tallies in the US election were altered by hacking." READ MORE

Source: Euronews

Date: 10 Jul 2018

Lebanese woman jailed in Egypt for Facebook video post

"A Lebanese tourist has been sentenced to eight years in prison by an Egyptian court for insulting Egyptians and their country in a video that she posted on Facebook. […] She claimed that she had been sexually harassed in the country. Having subsequently posted a video apologising for her original post and saying that she had not intended to offend Egyptians, Mona el-Mazbouh was arrested as she tried to leave the country in May. She was charged with "deliberately broadcasting false rumors which aim to undermine society and attack religions" and sentenced to 11 years in prison, a term subsequently reduced to eight years. Amnesty International told Euronews, however, that it had reviewed the original video and could confirm that it was a form of self-expression. Amnesty believes the video does not contain the incitement that is implied by the criminal charges brought against el-Mazbouh. Under the Egyptian constitution, the right to self-expression should ordinarily be protected." READ MORE

Source: Chatham House

Date: 4 Jul 2018

Cybercrime Legislation in the GCC Countries: Fit for Purpose?

"Most GCC countries have enacted or updated their cybercrime laws as part of their efforts to address the increasing threat of cybercrime. However, most of these focuses on limiting freedom of expression and at the same time omit key elements needed to combat cybercrime as this would be understood under most legal frameworks. […] Regarding their structure, cybercrime legal frameworks in the GCC are focused on substantive criminal law that criminalizes offences considered to be cybercrimes. However, in prosecutions and investigations, most GCC countries still apply traditional texts to cybercrime cases that are mostly oblivious to the nature of these cases. This impedes the success of these efforts and therefore the overall impact of fighting cybercrime. Regarding their content, all GCC countries, except for Bahrain, have introduced as part of their cybercrime laws provisions that criminalize a wide-spectrum of content, using vaguely worded provisions that create the potential for confusion and abuse. […] GCC governments would benefit extensively from joining international forums on cybercrime – such as the Budapest Convention – as this would help them in harmonizing and updating their laws, in enhancing their cybercrime investigative techniques, and in increasing international cooperation between them and with other countries." READ MORE

Source: Europol

Date: 11 Jul 2018

Two criminal groups dismantled for laundering EUR 2.5 million through smurfing and cryptocurrencies

"Europol has supported the Spanish Guardia Civil and the National Police of Colombia in dismantling two criminal organisations involved in large-scale money laundering. It is estimated that the EUR 2.5 million have been laundered by using different methods, such as smurfing and cryptocurrency exchanges. […] The group used cryptocurrency exchanges to convert large amounts of money from cash into cryptocurrencies, like Bitcoins and Altcoins, and later transferred them to other virtual wallets controlled by the Colombian organisation, which allowed the return of the illicit proceeds to South America, thus hiding the origin of the money." READ MORE

Source: Born 2 Invest

Date: 10 Jul 2018

Cryptojacking surpasses ransomware as top cyber crime

"A few years back, ransomware was one of the most common cyber crimes on the internet. Now, two cybersecurity firms have revealed that cryptojacking has grown immensely bigger. Cryptojacking is defined as "the unauthorized use of someone else's computer to mine cryptocurrency." Similar to ransomware, the attack is initiated when a person unknowingly opens or clicks on a malicious link sent by the attacker. […] According to Russia-based Kaspersky Lab, cryptojacking is the top cyber crime of 2018. Its data reveal that ransomware attacks have dropped significantly from 1,152,299 in 2016–17 to 751,606 in 2017–18. On the other hand, cryptojacking incidents have risen from 1.9 million to 2.7 million in the same time frame. McAfee Labs from California has the same findings with regards to cryptojacking. The crime grew by 629 percent, jumping from approximately 400,000 in the fourth quarter of 2017 to 2.9 million in the first quarter of 2018. The firm also indicated that ransomware attacks fell by 32 percent." READ MORE

Source: ZyCrypto

Date: 4 Jul 2018

Japanese Financial Authorities Set to Review Cryptocurrency Regulations

"The agency responsible for the security and maintenance of the Japanese financial sector, the Financial Service Agency (FSA) is considering to change the legal basis for how it regulates cryptocurrency exchanges in the region. […] This move has become imperative and necessary due to the incessant attacks on the virtual currency sector by hackers and fraudsters. Now, the regulators are looking to formulate new laws to safeguard the industry, improve customer satisfaction and confidence of investors in the crypto market in Japan. The new law and legislation have in a huge way reduced the gap between the traditional financial sector and cryptocurrency industry as the new bill tends to recognize cryptocurrency legally as electronic money." READ MORE

Source: IT Web Africa

Date: 12 Jul 2018

Collaborate or bust – Africa needs to coordinate response to cybercrime

"Countries in Africa have been urged to establish Computer Incident Response Teams (CIRT) and Cybersecurity Emergency Response Teams (CERT) to tackle an increase in cybercrime. According to Africa Cybersecurity Report 2017 by Serianu, cybercrime cost the continent US$ 3.5 billion in 2017. Speaking at the Africa Cyber Defense Summit in Nairobi, Kaleem Usmani, Head of Mauritian CERT National Computer Board, said that only 18 out of 54 African countries have set up their response teams, leaving the majority without the ability to co-ordinate a response in the event of a cyber attack. Usmani said for a continent of over 450 million internet users, the number of CIRT and CERT teams is low. "These are the teams that help governments look at cyber security matters and find a fix."." READ MORE

Source: TASS

Date: 6 Jul 2018

About 40,000 cybercrimes committed in Russia in 2018 — police

"Russia's Interior Ministry has registered about 40,000 cybercrimes in Russia since the beginning of the year of 2018, Deputy Interior Minister Igor Zubov told reporters on Friday. "About 40,000 [cybercrimes] have been registered. The damage is not big, but most of them are targeting banks. The cyber-attack hits, they repel it but prefer not to spread this information as latency is rather high," Zubov said." READ MORE

Source: L'Orient-le Jour

Date: 13 Jul 2018

Le Liban est l'un des pays les plus vulnérables face aux cybercrimes

"De scandale en scandale, le Liban a fini par révéler au grand jour sa vulnérabilité face aux attaques et aux crimes commis sur son cyberespace et dont la sophistication dépasse de loin les capacités défensives de l'État, quasi inexistantes. […] Le Liban doit absolument mettre les bouchées doubles pour pallier ce manque. L'absence de législation pose un problème sérieux à la justice qui doit aujourd'hui faire face à un domaine qui n'est pas codifié par la loi. Si l'on revient à la Constitution, il y est clairement mentionné, à l'article 8, qu'« aucune infraction et aucune peine ne peuvent être établies que par la loi ». De même, « nul ne peut être arrêté ou détenu que suivant les dispositions de la loi ». C'est le cas notamment dans l'affaire de la dernière cyber attaque, les juges n'ayant pas de texte pour se prononcer." READ MORE

Source: Financial Watch Nigeria

Date: 3 Jul 2018

Minister raises alarm on Cyber-related threats to Nigeria

"Cyber-related threats to Nigeria and the West African region are increasing in number, type and sophistication, the Minister of Communication, Mr Adebayo Shittu, has said. […]. He also disclosed that the ministry was working with the Office of the National Security Adviser and the National Assembly to reinforce or build international norms to regulate adverse state behaviour on the cyberspace. "We will continue to partner ONSA to build capacity to benefit from the Internet, to secure it, and to engage with international rule-making. The cyber ecosystem has been 'weaponised' and manipulated to devastating effect to undermine democratic processes, influence voting in elections and whip up tension and divisions between and among societal groups." […] According to the minister, the Ministry of Communications, in conjunction with relevant stakeholders, is coming up with an essential and effective cyber-security management strategy based on existing legislative frameworks, while building on the work already being done by bodies like the Cybercrime Advisory Council." READ MORE

Source: The Southern Times

Date: 2 Jul 2018

Botswana businesses hit by cybercrime

"Botswana police have indicated that there is marked increase in cases of crime involving the Internet, in which businesses in Botswana have been swindled of money through the use of the Internet or social media. Botswana Police Service spokesperson, Near Bagali, said of late their offices countrywide have been inundated with reports of companies and individuals swindled of their money through cyber-facilitated crimes. He said the cyber-related crimes range from suspected criminals hijacking on-going business transactions to divert payments into cybercriminals' accounts. According to Bagali, the criminals send an email to the customer using the supplier's compromised email account or an email, which looks similar to a legitimate email account, to inform them about the change of bank account to the account controlled by the cybercriminals." READ MORE

Latest reports

- Council of Europe, Mapping study on cyberviolence, 9 Jul 2018
- Council of Europe, Template for Mutual Legal Assistance Request for subscriber information under Article 31, 9 Jul 2018
- Council of Europe, Template for Data Preservation Request under Articles 29 and 30, 9 Jul 2018
- European Parliament, European production and preservation orders and the appointment of legal representatives for gathering electronic evidence, July 2018
- ICANN, Data Protection/Privacy Update: Additional Guidance from the European Data Protection Board, 13 Jul 2018
- ECPAT, Sexual Exploitation of Children in Lao PDR, published on 5 Jul 2018
- PwC, 2018 Global Economic Crime and Fraud Survey, June 2018
- Marketing.Science, Report on ad fraud and cybercrime 2018, July 2018
- The Times of India, Number of cybercrimes across India in 2017 - Infographic, 7 Jul 2018

Upcoming events

- 16 – 20 July 2018 – Study Visit of the Nepalese Attorney General Office to European Union Institutions (e.g. Eurojust) and national judicial authorities in the Netherlands, Belgium and Romania, GLACY+
- 16 – 20 July 2018, Accra, Ghana – Advanced Judicial Training on cybercrime and Electronic evidence for judges, prosecutors and lawyers with participation of Anglophone countries from the ECOWAS Region, GLACY+
- 17 – 28 July 2018, Leon, Spain – Participation in the Cyber Security Summer Bootcamp 2018, GLACY+
- 23 – 25 July 2018, Bucharest, Romania – First preparatory meeting to develop a Cyber Exercise Scenario, iPROCEEDS
- 30 July – 3 August 2018 – Adaptation of the Basic Judicial Training on Cybercrime and Electronic Evidence, Strasbourg, France, CyberSouth

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