Cybercrime Digest

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

16-31 May 2019

Source: Council of Europe

Date: 27 May 2019

Cooperation on cybercrime in the Pacific: PILON meets in Vanuatu

"The 3rd meeting of the Cybercrime Working Group of the Pacific Island Law Officers Network (PILON) is focusing on the international sharing of electronic evidence. In the opening session of the regional meeting, Leotrina Macomber, Chair of the PILON Cybercrime Working Group, noted that geographical isolation did not make the Pacific region immune to cybercrime. Creating the ability for Pacific Island States to share electronic evidence must remain a priority. Stephen Bouwhuis, from the Attorney General's Department of Australia, stressed the relevance of this PILON workshop for cooperation against cybercrime between all participating partners and States. Justice Daniel Fatiaki pointed at the increasing importance of electronic evidence in Vanuatu for any type of offence, including, for example, cases of family violence. […] The chair of the Cybercrime Convention Committee, Cristina Schulman, underlined the need for legislation on cybercrime and electronic evidence as the foundation for criminal justice and the rule of law in cyberspace. She welcomed that most Pacific Island States are developing such legislation and are considering accession to the Budapest Convention on Cybercrime. The Council of Europe is prepared to support this process." READ MORE

Source: Council of the European Union

Date: 17 May 2019

Cyber-attacks: Council is now able to impose sanctions

"On 17 May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP). Cyber-attacks falling within the scope of this new sanctions regime are those which have significant impact and which: (i) originate or are carried out from outside the EU or (ii) use infrastructure outside the EU or (iii) are carried out by persons or entities established or operating outside the EU or (iv) are carried out with the support of person or entities operating outside the EU." READ MORE

Source: DAC Beachcroft

Date: 22 May 2019

Overseas Production Orders, new powers for UK LEAs to compel disclosure of electronic data stored abroad

"On 12 February 2019, the Crime (Overseas Production Orders) Act 2019 came into force. Its aim is to assist law enforcement agencies speed up the process of obtaining disclosure of electronic data stored outside of the UK for use in criminal and regulatory investigations and prosecutions in the UK. Whilst the Act is in force, it is not yet capable of being used by law enforcement agencies because it can only operate where there are, in place, "designated international co-operation arrangements" which provide for mutual assistance in connection with investigation or prosecution of offences. Such designated co-operation arrangements will, in time, be ratified and designated by the Secretary of State. It is understood the first such designated co-operation agreement is likely to be agreed between the UK and the US." READ MORE

Source: Europol

Date: 22 May 2019

Multi-million Euro cryptocurrency laundering service bestmixer.io taken down

“Today, the Dutch Fiscal Information and Investigation Service (FIOD), in close cooperation with Europol and the authorities in Luxembourg, clamped down on one of the world’s leading cryptocurrency mixing service Bestmixer.io. Initiated back in June 2018 by the FIOD with the support of the internet security company McAfee, this investigation resulted in the seizure of six servers in the Netherlands and Luxembourg. Bestmixer.io was one of the three largest mixing services for cryptocurrencies and offered services for mixing the cryptocurrencies bitcoins, bitcoin cash and litecoins. The service started in May 2018 and achieved a turnover of at least $200 million in a year’s time and guaranteed that the customers would remain anonymous. […] A cryptocurrency tumbler or cryptocurrency mixing service is a service offered to mix potentially identifiable or 'tainted' cryptocurrency funds with others, so as to obscure the trail back to the fund's original source. The investigation so far into this case has shown that many of the mixed cryptocurrencies on Bestmixer.io had a criminal origin or destination.” READ MORE

Source: EDN Hub

Date: 17 May 2019

US, EU spar over sharing electronic evidence in investigations

“In the European Union, 85 percent of criminal investigations involve electronic evidence, of which two-thirds is stored in another country. But obtaining potential evidence from Facebook account today takes Europeans on average ten months. A European investigating judge must ask an official of his government to send an official request to the US government. Then a US judge, who isn’t familiar with the case, then makes the request to Facebook. The FBI then reviews the evidence to ensure it does not contain confidential information unrelated to the original request. The data is then sent to the requesting government, which passes it to the investigators. “This doesn’t work, the operations are totally blocked,” a frustrated European justice official said. “We all know that virtually every serious threat we investigate today requires access to electronic evidence like the contents of emails, instant messages, photos, traffic data, session logs, subscriber information, and the like,” Richard Downing, a top US Justice official, said in a speech in London last month. “Our collective safety and security depends on our ability to maintain lawful and efficient cross-border access to that evidence.”” READ MORE

Source: NATO CCDCOE

Date: 29 May 2019

An interactive cyber law toolkit launched by the NATO CCDCOE in Tallinn

“The Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence has launched an interactive web-based resource for legal professionals and students, called the Cyber Law Toolkit. […] The toolkit is a dynamic interactive web-based resource for legal professionals and students who work with wide array of topics related to international law and cyber operations. “The practical toolkit consists of several hypothetical scenarios, each of which contains a description of cyber incidents inspired by real-world examples and accompanied by detailed legal analysis,” the centre said. “The aim of the analysis is to provide throughout examination of the applicability of international law to the diverse scenarios and related legal issues.” READ MORE

Source: RPC

Date: 16 May 2019

UK, only 1% of cybercrime prosecuted, claim lawyers

"Over 17,900 incidences of computer hacking reported in the UK in 2018. However, despite the rise last year, the number of prosecutions still represents less than 1% of reported cybercrimes in the UK. […] Richard Breavington, Partner at RPC, says: "Cybercrime has become accepted as a low-risk, potentially high-reward activity for organised criminals. If they act professionally, they can make substantial sums of money with very little chance of being caught. Understandably the priorities for policing cybercrime have been in areas which have a potential nation state impact. A result is that the rise of less sensitive cybercrime has gone largely unchecked and it has been left largely to the private sector to deal with."" READ MORE

Source: European Union External Action Service

Date: 21 May 2019

EU statement on the occasion of 28th session of the CCPCJ, Vienna 20-24 May 2019

"[…] We are deeply concerned that transnational organised crime and corruption undermine human development, the rule of law, transparency, fair competition and democracy, damage private and public sector integrity and reduce access to public services. We reaffirm the importance of the United Nations Convention against Transnational Organized Crime (UNTOC) and the Protocols thereto as well as the United Nations Convention against Corruption (UNCAC). We welcome the work of UNODC to assist Member States in the full and effective implementation of these conventions. […] Combating cybercrime represents a very special challenge demanding an even better international cooperation. At the same time, we remain strongly committed to a free, open and secure internet respecting human rights and fundamental freedoms. We promote the Budapest Convention on Cybercrime as the framework for international cooperation and we join the broad international consensus on the need to increase our capacity building efforts." READ MORE

Source: Buzzfeed News

Date: 24 May 2019

Facebook Removed Over 2 Billion Fake Accounts, But The Problem Is Getting Worse

"Despite recent enforcement actions, Facebook is still plagued by fake accounts, including thousands helping promote a far-right German political party. Facebook announced this week it removed 2.19 billion fake accounts between January and March, its biggest-ever takedown of fakes in a single quarter. Company CEO Mark Zuckerberg confidently told media that "we're taking down more fake accounts than ever." What he didn't say is that there are also more active fake accounts on Facebook than there were six months ago — more than ever before. Facebook now says 5% of active accounts are fake, up from its previous estimate of 3% to 4%." READ MORE

Source: enSilo

Date: 24 May 2019

New APT10 Activity Detected in Southeast Asia

"In April 2019, enSilo detected what it believes to be new activity by Chinese cyber espionage group APT10. The variants discovered by enSilo are previously unknown and deploy malware that is unique to the threat actor. These malware families have a rich history of being used in many targeted attacks against government and private organizations. The activity surfaced in Southeast Asia (Philippines), a region where APT10 frequently operates." READ MORE

Source: Le 20 Heures

DatCarnegiee: 23 May 2019

Cybercriminalité : le Maroc est-il sécurisé ?

"Le Royaume du Maroc ,classé parmi les pays les plus exposés à la menace électronique, estdevenu conscient de ce phénomène . Il a mis en place une stratégie nationale de cybersécurité et de sécurité des systèmes d'information . Plusieurs mesures ont été réalisés sur le plan organisationnel et réglementaire enmatière de lutte contre la cybercriminalité. Sur le plan organisationnel ,le Maroc amis en place la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), le Centre Marocain d'Alerte et de Gestion des Incidents Informatiques (MA-CERT) relevant de la Direction de la Défense Nationale, des Laboratoires Régionaux d'Analyse de Traces Numériques et Anti-cybercriminalité, relevant de la Direction Générale de la Sûreté Nationale (DGSN), et également la Commission Nationale de Contrôle de la Protection des Données Personnelles (CNDP), réorganisée dernièrement. […] L'adhésion du Maroc à la Convention de Budapest sur la cybercriminalité a placé le Royaume parmi les pays leaders en matière de la sécurité cybernétique , tout en lui permettant de se doter d'un mécanisme performant pour faire face aux crimes commis via les systèmes informatiques." READ MORE

Source: GhanaWeb

Date: 29 May 2019

Ghana, Government to launch platforms for reporting cybercrimes, cybersecurity breaches

"Government is establishing various platforms to encourage people to report incidents of cybercrime and cyber-security breaches. "These channels will include online portals, hotlines, SMS lines, and dedicated app [mobile applications] that will be dedicated solely for incident reporting", Communication Minister Ursula Owusu-Ekuful explained. She said these channels will be launched in the coming weeks by the Ministry in collaboration with the Cyber Security Centre, Ghana Police, telecom service providers and the Internet Watch Foundation (IWF). The initiative is geared towards ensuring the proper handling of crimes perpetuated online and forms part of the implementation of Child Online Protection (COP)." READ MORE

RELATED ARTICLES

GhanaWeb, CID to establish Digital Forensic Laboratory, 28 May 2019

Source: IT Web

Date: 29 May 2019

South Africa is 'safe haven for cyber criminals'

"In the absence of legislation that addresses cyber crimes, South Africa has become a safe haven for cyber criminals, said Corien Vermaak, cyber security specialist at Cisco. […] In 2015, the Department of Justice and Constitutional Development (DOJ) initiated the process to establish decisive policy in the form of the Cyber Crimes Bill, responding to the country's lack of legislation addressing cyber crimes. Initially dubbed the Cyber Crimes and Cyber Security Bill, the piece of legislation received backlash, with several critics saying it was too broad, open to abuse and threatened the fundamental democratic spirit of the Internet. After multiple reiterations and drafts, the Bill was revised and the DOJ tabled a new version before Parliament's Portfolio Committee on Justice and Correctional Services in October 2018. Last November, the Bill was passed by the National Assembly, and transferred to the National Council of Provinces for agreement, whereby it will eventually reach the president to be signed into law." READ MORE

Source: New Zealand Government

Date: 16 May 2019

The Christchurch call to eliminate terrorist and violent extremist content online

"French President Emmanuel Macron and New Zealand Prime Minister Jacinda Ardern have led a group of world leaders, tech companies and organisations to adopt a pledge that seeks to eliminate terrorist and violent extremist content online to stop the internet being used as a tool for terrorists. The Christchurch Call, named for the New Zealand city in which 51 members of its Muslim community were murdered in a live-streamed terrorist attack on March 15, took place in Paris today and saw leaders from 10 countries and major tech companies commit to a set of collective actions that aim to eliminate terrorist and violent extremist content online. The Christchurch Call is an action plan that commits government and tech companies to a range of measures, including developing tools to prevent the upload of terrorist and violent extremist content; countering the roots of violent extremism; increasing transparency around the removal and detection of content, and reviewing how companies' algorithms direct users to violent extremist content." READ MORE

Latest reports

- European Union, Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, 10 May 2019
- U.S. Department of Justice, "What the CLOUD Act does and does not do", 16 May 2019
- Australian Strategic Policy Institute, Hacking democracies – Cataloguing cyber-enabled attacks on elections, 15 May 2019
- Carnegie Endowment for International Peace, Papers of the Encryption Working Group, 30 May 2019
- International Committee of the Red Cross, Potential human costs of cyber operations, 29 May 2019
- APWG, Phishing Activity Trends Report – First Quarter 2019, May 2019

Upcoming events

- 3-7 June, Santo Domingo, Dominican Republic – Cryptocurrency investigations training to Police Cyber-units, GLACY+
- 3-7 June, Dakar, Senegal – Regional training of trainers for first respondents on cybercrime and electronic evidence to the African gendarmeries, GLACY+
- 10-14 June, Tunis, Tunisia – Adaptation of the judicial training curricula for the national context, CyberSouth
- 12-13 June, Tirana, Albania – Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (2nd part), iPROCEEDS
- 12-14 June, Santo Domingo, Dominican Republic – Regional conference on cybercrime and cyber security policies and strategies, GLACY+
- 12-14 June, Bucharest, Romania – Euromed Justice Joint Conference, 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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE