Cybercrime Digest

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

16-31 October 2018

Source: U.S. Department of State

Date: 16 Oct 2018

EU-U.S. Cyber Dialogue Joint Elements Statement

"On the occasion of the fifth meeting of the EU-U.S. Cyber Dialogue in Brussels on 10 September 2018, the European Union (EU) and United States reaffirmed their strong partnership in favour of a global, open, stable and secure cyberspace where the rule of law fully applies, where the same rights that individuals have offline are protected online, and where the security, economic growth, prosperity, and integrity of free and democratic societies is promoted and preserved. […] The EU and United States reaffirmed their strong commitment to human rights and fundamental freedoms online and condemned undue restrictions on freedom of expression and censorship in violation of international human rights law. […] The EU and United States also underlined the need to address the digital divide to enable economic growth, social development, and increasing cyber resilience towards cyber threats and stressed their commitment to continued capacity building assistance to this end, including through the Global Forum for Cyber Expertise. […] The EU and United States reaffirmed the importance of the Budapest Convention as a basis for national legislation and international cooperation in fighting cybercrime." READ MORE

Source: GhanaWeb

Date: 22 Oct 2018

Ghana, Parliament to ratify Budapest Convention on Cybercrime

"Speaking at the climax of the Cybersecurity Awareness and a safer Digital Ghana campaign Month, President Akufo-Addo assured that the government is making efforts to push for parliament to ratify the deal when the House resumes. "As a government, we have signed both the Malabo and Budapest Convention which sets the tone for Ghana to implement initiatives on cybersecurity. I'm happy to announce that when parliament resumes, one of the first sets of laws to ratify is the Budapest Convention. As you're all aware, Ghana is the third nation on the African continent to sign these two conventions and the government is committed to implementing it to the latter" President Akufo-Addo said." READ MORE

RELATED ARTICLE

New Ghana, Ghana Officially Opens Judicial Training On Cybercrime And Electronic Evidence For Supreme Court Judges, 24 Oct 2018

Source: DW

Date: 2 Nov 2018

Hackers obtain nuclear power plant plans in France

"Thousands of sensitive documents pertaining to nuclear power plants, prisons and tram networks have been stolen from the servers of a French company in a cyberattack. […] A spokeswoman from Ingerop said more than 11,000 files from a dozen projects were obtained. They were said to include plans showing the planned locations of video cameras for a French high-security prison, documents about a planned nuclear-waste dump in northeastern France and personal information on more than a thousand Ingerop workers. Some of the documents were connected with the Fessenheim nuclear plant on the border to Germany, reports said." READ MORE

Source: The Independent

Date: 16 Oct 2018

UK to be hit by 'category 1' cyber emergency, intelligence chief warns

"Britain will be hit by a life-threatening "category 1" cyber emergency in the near future, the National Cyber Security Centre (NCSC) has warned. The NCSC's annual review revealed it is currently repelling around 10 attempted cyber attacks every week, with "hostile states" said to be responsible for the bulk of thwarted strikes. Since it became fully operational two years ago, the centre's teams have dealt with 1,167 cyber incidents. […] He added: "I remain in little doubt we will be tested to the full, as a centre, and as a nation, by a major incident at some point in the years ahead, what we would call a category 1 attack." The NCSC defines a category 1 incident as an attack which causes "sustained disruption" of essential services or affects national security, leading to severe economic or social consequences, or to loss of life." READ MORE

Source: ITNews

Date: 23 Oct 2018

Banks need mandatory cyber security tests says RBA, EU Central Bank

"Banks could soon face penetration tests instigated by regulators and be subject to the equivalent of an annual cyber-roadworthy certificate under bold reforms canvassed by the Reserve Bank of Australia, JP Morgan and the European Central Bank at SIBOS 2018 in Sydney. In a discussion dedicated to addressing cyber risk, some of the world's leading central financial authorities and institutions frankly admitted much more must be done than just creating frameworks and relying on commercial solutions if all financial players are going to be secured." READ MORE

So Source: Pressafrik

Date: 23 Oct 2018

L'accès transfrontalier aux données numériques et la lutte contre la cybercriminalité: Quels enjeux pour l'Afrique?

"De nos jours, il est devenu banal en Afrique d'utiliser les médias sociaux et les services et applications de messagerie électronique pour communiquer, travailler, socialiser ou obtenir des informations. Cependant, ils peuvent aussi être utilisés à mauvais escient pour commettre ou faciliter à perpétrer des actes cybercriminels, y compris des crimes graves tels que des attaques terroristes. Or, dans la plupart des enquêtes pénales impliquant la cybercriminalité, les autorités judiciaires ont besoin d'accéder à des données susceptibles de servir de preuves (e-mail, heure de connexion, identité du titulaire d'un compte mail, photos ou vidéos de pornographie enfantine, etc.) et qui sont stockées dans les serveurs des fournisseurs de services (Facebook, Gmail, Yahoo, Apple, Google, Microsoft, etc.) établis dans d'autres États, en particulier aux Etats-Unis. […] Cependant, les preuves numériques dans le cloud présentent des particularités technologiques, en raison notamment de l'ubiquité et de la nature décentralisée de l'architecture du « nuage ». […] Les données sont parfois dupliquées et fragmentées sur des serveurs différents localisés dans plusieurs Etats afin de les préserver. Les structures d'investigation se heurtent souvent à l'impossibilité technique de localiser le lieu de stockage des données numériques. Ainsi, les mécanismes classiques de coopération dont les principes de base ont été fixés depuis plusieurs dizaines d'années dans le cadre d'un environnement matérialisé, sont de plus en plus mis à rude épreuve. " (Papa Assane TOURE) READ MORE

Source: Stockholm Center for Freedom

Date: 26 Oct 2018

UN panel to Turkish gov't: Prosecution based on alleged use of ByLock violates civil and political rights

"The UN Human Rights Council's Working Group on Arbitrary Detention (UN/WGAD) has stated in a recently released assessment that detention, arrest and conviction in Turkey based on the alleged use of the ByLock mobile phone messaging application is a violation of Articles 19, 21 and 22 of the International Covenant on Civil and Political Rights. Turkish authorities believe ByLock is a communication tool among alleged followers of the Gülen movement. Tens of thousands of people, including civil servants, police officers, soldiers, businessmen, and even housewives have either been dismissed or arrested for allegedly using ByLock since a controversial coup attempt on July 15, 2016. UN/WGAD examined an application submitted by the lawyers for Mestan Yayman and released its opinion on the case. Yayman, who used to be vice governor of Antalya province, was suspended on August 29, 2016, and was subsequently dismissed from his job under Statutory Decree No. 672, issued on September 1, 2016, under which about 50,000 people were dismissed. […] Turkey has suspended or dismissed about 170,000 judges, teachers, police and civil servants since July 15, 2016. On December 13, 2017, the Justice Ministry announced that 169,013 people have been the subject of legal proceedings on coup charges since the failed coup. Turkish Interior Minister Süleyman Soylu announced on April 18, 2018, that the Turkish government had jailed 77,081 people between July 15, 2016, and April 11, 2018, over alleged links to the Gülen movement. " READ MORE

RELATED ARTICLE: Opinions adopted by the Working Group on Arbitrary Detention at its eighty-second session, 20–24 August 2018

Source: ZD Net

Date: 16 Oct 2018

Czech intelligence service shuts down Hezbollah hacking operation

"The Czech Security Intelligence Service (BIS) has intervened and taken down servers that have been used by Hezbollah operatives to target and infect users around the globe with mobile malware. […] BIS said the servers were located in the Czech Republic, and the agency was "almost certain" they were operated by Hezbollah, an Islamist political party and militant group based in Lebanon, which the US and fellow NATO countries have labeled as a terrorist organization. […] Hezbollah operatives operated by creating Facebook profiles, posing as attractive women, and reaching out to selected targets. The goal of the operation was to engage the target in private discussions and convince it to install a third-party instant messaging application to continue the conversation via this second, malware-infested app." READ MORE

Source: Ministerio del Interior y Seguridad Publica

Date: 25 Oct 2018

Chile, Gobierno envía proyecto de Ley de Delitos Informáticos

"Junto con la iniciativa legal, el Presidente de la República firmó un Instructivo Presidencial, estableciendo las obligaciones para los distintos servicios públicos del Estado para robustecer los sistemas de ciberseguridad. […] El texto enviado hoy al Congreso Nacional reemplazará a la actual normativa – promulgada en 1993 – y forma parte de la Estrategia Nacional de Ciberseguridad para cuya implementación se nombró en calidad de Delegado Presidencial a Jorge Atton." READ MORE

Source: Escuela Nacional de la Judicatura

Date: 25 Oct 2018

Escuela Nacional de la Judicatura celebra Congreso en Cibercriminalidad y Evidencia Digital en la República Dominicana

"La Escuela Nacional de la Judicatura (ENJ), realizó la apertura del primer Congreso Internacional sobre Cibercriminalidad y Evidencia Digital, donde participan expertos nacionales e internacionales durante los días 25 y 26 de octubre del presente año. […] El congreso, representa un espacio para analizar el crecimiento acelerado de los delitos que se cometen a través de las tecnologías de la información y la comunicación. Entre los temas desarrollados en el congreso estuvieron la red oscura y cibercrimen; pornografía infantil; ciberacoso y sexting; debido proceso y las reglas de evidencia en el campo del cibercrimen; los órganos de prevención y persecución del cibercrimen en la República Dominicana, entre otros." READ MORE

Source: Bloomberg

Date: 19 Oct 2018

WhatsApp Bans More Than 100,000 Accounts in Brazil Election

"WhatsApp banned hundreds of thousands of accounts in Brazil as the Facebook Inc. messaging service struggles to contain spam, misinformation and political shenanigans ahead of a runoff election in Latin America's largest country. Facebook set up a "war room" to stem the tide of hate speech, false information and other damaging content during Brazil's election this month, marking a test for the social network ahead of the November midterm elections in the U.S. While the company said it was able to thwart false information on its main social network, it's had more trouble controlling misbehavior on WhatsApp, which is encrypted and virtually impossible to monitor." READ MORE

Source: No More Ransom Project

Date: 26 Oct 2018

Pay No More: universal GandCrab decryption tool released for free on No More Ransom

"As of today, victims of the GandCrab ransomware can recover their files without giving into the demands of the criminals thanks to a new decryption tool released for free on www.nomoreransom.org. This data recovery kit was developed by the Romanian Police in collaboration with its counterparts from Bulgaria, France, Hungary, Italy, Poland, the Netherlands, United Kingdom and United States, together with the security company Bitdefender and Europol." READ MORE

Source: ENISA and Europol

Date: 25 Oct 2018

The importance of securing the Internet of Things

"Our world is hyper-connected now. Current estimates are that there are around 10 billion electronic devices with access to the internet and that number will have at least doubled by 2020. In addition to the many advantages and opportunities, the emerging ability of connected devices to impact the physical world has also created a new set of vulnerabilities and possibilities of exploitation by criminals. […] Crime scenes are changing because of the IoT: data from connected doorbells, cameras, thermostats, fridges, etc. can provide useful and crucial evidence. The necessary forensic techniques and training will need to be used to safeguard this data. Big data collected by IoT devices will become an integral part of a criminal investigation but also require the necessary means to protect the privacy of citizens." READ MORE

Source: Bleeping Computer

Date: 24 Oct 2018

Cathay Pacific Suffers Data Breach Impacting 9.4 Million Passengers

"The Cathay Pacific airline announced today that a system containing passenger data for up to 9.4 million passengers was breached by attackers. […] In a security notice, the airline has stated that the following information has been accessed: "The following personal data was accessed: passenger name; nationality; date of birth; phone number; email; address; passport number; identity card number; frequent flyer programme membership number; customer service remarks and historical travel information." READ MORE

Latest reports

- Europol and European Banking Federation, Click here and see how your money disappears – criminal #CyberScams of the 21st century, 16 Oct 2018
- Council of Europe, African Forum on Cybercrime – Website, October 2018
- Derechos Digitales, El Convenio de Budapest en América Latina, October 2018
- Harvard Kennedy School – Belferd Center for Science and International Affairs, Harvard Kennedy School, Can Democracy Survive in the Information Age?, October 2018
- Anti-Phishing Working Group (APWG) and the Messaging, Malware and Mobile Anti - Abuse Working Group (M3 AAWG), ICANN GDPR and WHOIS, Users Survey, October 2018
- Saudi Gazette, Cost of cybercrime to double to $6trn by 2021, 23 Oct 2018

Upcoming events

- 1 – 2 November 2018, Kyiv, Ukraine – Advisory Mission on international cooperation through 24/7 points of contact and mutual legal assistance, Cybercrime@EAP2018
- 5 – 7 November 2018, Budapest, Hungary – Training on financial frauds and virtual currencies in cooperation with the International Training Centre, International College of Financial Investigations, iPROCEEDS
- 5 – 9 November 2018, Chile - Introductory Judicial ToT on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers and adaptation of materials to the local context, GLACY+
- 7 – 8 November 2018, Algiers, Algeria – Study visit at specialized units, CyberSouth
- 12 – 14 November 2018, Tunis, Tunisia – Basic judicial Training, CyberSouth
- 12 – 14 November 2018, Bucharest, Romania – Regional workshop on Business E-mail Compromise, credit card fraud and e-commerce fraud, CyberSouth
- 12 – 15 November 2018, Bucharest, Romania - Regional case simulation exercise on cybercrime and financial investigations, iPROCEEDS
- 12 – 15 November 2018, Morocco - ECTEG Course, Cybercrime and digital forensics specialized training for law enforcement officers, GLACY+
- 12 – 15 November 2018, Senegal - Advanced Judicial Training on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers with participation of Francophone and Lusophone countries from the ECOWAS Region, GLACY+
- 13 November 2018, the Netherlands – Presentation on the Budapest Convention at the ENISA-EC3 Workshop on CSIRT and international law enforcement cooperation, GLACY+
- 13 – 14 November 2018 , Bucharest, Romania – Seminar "Investigating Web 2.0 - The Collection of Evidence Located Abroad and the Challenges of Transborder Access to Data", organized by ERA and NIM (National Institute for Magistracy), GLACY+

- 14 – 16 November 2018, Sri Lanka – In Country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strength the 24/7 points of contact for cybercrime and electronic evidence, GLACY+
- 15 November 2018, Beirut, Lebanon - Round table on cybersecurity strategy, CyberSouth
- 15 – 16 November 2018, Bucharest, Romania - Human Rights Workshop with the Fundamental Rights Agency, GLACY+
- 16 November 2018, Beirut, Lebanon – Awareness meeting on Budapest Convention and its instruments, CyberSouth

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime