Cybercrime Digest

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

16-31 January 2019

Source: Congreso de la Repùblica, Peru

Date: 31 Jan 2019

Perú se adhiere al Convenio de Budapest para combatir la ciberdelincuencia

"La Ciberdelincuencia es un problema que ha ido agravándose en los últimos años conforme el avance de la tecnología, en los que se han perpetrado múltiples delitos informáticos a nivel internacional. Ante esta preocupante situación, la Comisión de Relaciones Exteriores del Congreso, propuso mediante un proyecto de ley –aprobado anoche de manera unánime por el Poder Legislativo- la adhesión de nuestro país al Convenio de Budapest, lo que nos permitirá aplicar programas técnicos para enfrentar esta modalidad delictiva. […] El Convenio tiene como principal objetivo el desarrollo de una política criminal a nivel internacional frente a la Ciberdelincuencia, mediante la homologación de la legislación penal, sustantiva y procesal, así como el establecimiento de un sistema eficaz eficiente y en tiempo real de cooperación internacional, además de mejorar las capacidades de investigación de los delitos contemplados en el referido convenio, explicó." READ MORE

RELATED ARTICLES

Council of Europe, Peru: accession to Budapest Convention approved, 30 Jan 2019

Source: Politico

Date: 16 Jan 2019

Europe's most hackable election

"The election — in which voters in 27 countries will install a new European Parliament and by extension a new crop of top EU officials — is uniquely vulnerable, officials say. "Given the dispersed nature and comparatively long duration of the European Parliament elections, they present a tempting target for malicious actors," European Commissioner for Security Julian King told POLITICO. […] The "European election" is in fact a series of simultaneous elections that will take place on May 23-26, in which the integrity of the vote depends on how 27 national governments fend off hackers and other threats. And while some governments are better prepared than others, it would only take one successful act of disruption to cast doubt on the composition of the next European Parliament. "A successful campaign against one member state that includes cyber-enabled elements could mean that the assignment of seats cannot be confirmed thus compromising the entirety of election processes," said a recent EU report into the cyber risks to the election. A security incident "could impact the ability of the European Parliament to convene and thus could affect the very functioning of the European Union." Threats to the integrity include disinformation campaigns, cybersecurity breaches and digital tampering with the outcome of the votes" READ MORE

Source: ICANN

Date: 29 Jan 2019

GDPR and WHOIS, ICANN Board Reaffirms Temporary Specification for gTLD Registration Data

"The Board of Directors of ICANN voted this week to reaffirm the "Temporary Specification for gTLD Registration Data" for an additional 90 days. […] Under the procedures for adopting Temporary Policies, the Board must reaffirm the adoption every 90 days, and may continue to do so for no more than a year." READ MORE

Source: Le Monde

Date: 21 Jan 2019

Données personnelles : la CNIL condamne Google à une amende record de 50 millions d'euros

"[…] Cette condamnation intervient après les plaintes collectives, qui ont fédéré plus de 10 000 signataires, déposées devant la CNIL par les associations None of Your Business et La Quadrature du Net (QDN), alors que le règlement européen pour la protection des données (RGPD) venait tout juste d'entrer en vigueur en Europe, le 25 mai 2018. Un texte censé permettre aux citoyens européens de conserver la maîtrise de leurs données personnelles, notamment face aux géants du numérique, qui, comme Google, les utilisent à des fins commerciales." READ MORE

Source: Department of Justice and Equality, Ireland

Date: 17 Jan 2019

Ireland, Minister Flanagan makes a statement on the Budapest Convention on Cyber Crime

"I will provide an update in relation to ratification of the Cybercrime Convention, otherwise known as the Budapest Convention, which Ireland signed on 28 February 2002. Much work has been done on implementing the provisions of the Convention in the meantime, notwithstanding unforeseen delays along the way, largely reflecting developments at European level. […] It is important to first point out that the vast majority of the provisions in the Cybercrime Convention are already provided for in Irish law. The Deputy will be aware that it is necessary to give effect to legal provisions in international instruments in national law before the ratification process can be finalised. The most significant development towards ratification of the Convention was enactment in 2017, by this Government, of the first piece of legislation in this jurisdiction specifically dedicated to dealing with cybercrime. […] I am pleased to inform the House that the current Government Legislation Programme makes provision for the drafting of a new Cybercrime Bill to give effect to those remaining provisions of the Cybercrime Convention not already provided for in national law in order to enable ratification of the Budapest Convention. Furthermore, a new area of responsibility for cybercrime has been established within my Department and one of the key priorities of this new area is to progress ratification of the Budapest Convention. To this end, officials recently attended a meeting of the Cybercrime Convention Committee in Strasbourg and held discussions with the Council of Europe Secretariat in order to progress outstanding issues for Ireland in relation to the Convention." READ MORE

Source: U.S. Department of Justice

Date: 30 Jan 2019

U.S. Justice Department announces Court-Authorized efforts to map and disrupt botnet used by North Korean hackers

"The Justice Department today announced an extensive effort to map and further disrupt, through victim notifications, the Joanap botnet – a global network of numerous infected computers under the control of North Korean hackers that was used to facilitate other malicious cyber activities. This effort targeting the Joanap botnet follows charges unsealed last year in which the United States charged a North Korean citizen, Park Jin Hyok, a member of a conspiracy backed by the North Korean government that carried out numerous computer intrusions. Those charges alleged that the conspiracy utilized a strain of malware, "Brambul," which was also used to propagate the Joanap botnet." READ MORE

Source: Eurojust

Date: 28 Jan 2019

Cybercrime: xDedic illegal online marketplace dismantled

"On 24 January, members of the National Police and the Prosecutor General's Office of Ukraine, with assistance from members of the Federal Computer Crime Unit (FCCU) of Belgium, Europol, and the US Federal Bureau of Investigation (FBI) and Internal Revenue Service (IRS) of Tampa, Florida, conducted house searches in nine places in Ukraine. Several IT systems were confiscated and three Ukrainian suspects were questioned. The house searches were related to two criminal investigations into the xDedic Marketplace, on which access to tens of thousands of compromised servers of unknowing victims (companies and private individuals) was offered for sale. The hacking was accomplished via the Remote Desktop Protocol (RDP). Buyers and sellers traded such RDP servers on this platform for amounts ranging from USD 6 to more than USD 10 000 each. In the first investigation, the investigating judge in Mechelen, at the request of the Belgian Federal Prosecutor's Office and the General Prosecutor's Office of Ukraine, conducted a criminal investigation. At the beginning of 2018, a JIT agreement was signed between Belgium, Ukraine, Eurojust and Europol, which was renewed early this year. The JIT was funded by Eurojust. The investigation focused on a number of vendors on the xDedic Marketplace, who sold a large number of Belgian hacked computer systems, and the organised criminal group (OCG) that organised and operated the illegal online marketplace." READ MORE

Source: Delegation of the European Union to Indonesia and Brunei Darussalam

Date: 22 Jan 2019

The EU Ambassador to Indonesia at the Workshop on Cybercrime and Electronic Evidence for Prosecutors of Indonesia, delivered by Filipino trainers

"The Global Action on Cybercrime Extended (GLACY+) brings us together today. […] Given the Philippine commitment and its rich experience in driving the fight against cybercrime forward together with international partners, the Philippines functions as a platform to promote triangular cooperation. With this model, it is possible to promote cooperation and exchange of good practices to entire regions, with the ASEAN region being of particular importance. This is fully in line with the 2017 ASEAN Declaration to Prevent and Combat Cybercrime, which calls to join efforts and to cooperate at the regional level in preventing and combating cybercrime. […] The Philippines acceded the Budapest Convention on Cybercrime in 2018. I am very pleased to see that Indonesia would like to take advantage of the wealth of expertise and knowledge gained by its neighbouring country Philippines and advocated for this workshop as a platform for learning and exchanging experiences." READ MORE

Source: Ministry of Foreign Affairs of Japan

Date: 18 Jan 2019

The 3rd ASEAN-Japan Cybercrime Dialogue

"This Dialogue was inaugurated in 2014 as a follow-up to the commitment made at the ASEAN-Japan Commemorative Summit in December 2013. The 3rd Dialogue is held to confirm the importance of Convention on Cybercrime (Budapest Convention) with ASEAN Member States, to exchange information on trends and lessons learned to combat cybercrime, and to discuss ASEAN-Japan cooperation on cybercrime, such as capacity building to fight against cybercrime and the direction of concrete activities to be funded by Japan-ASEAN Integration Fund (JAIF)." READ MORE

Source: Medium

Date: 17 Jan 2019

Facebook's Sputnik Takedown—In Depth Analysis

"Facebook removed almost 300 pages from its platform for "coordinated inauthentic behavior" across the former-Soviet space on January 17, 2018. The pages masqueraded as groups with special interests—ranging from food to support for authoritarian presidents—and amplified content from the Kremlin's media agency, Rossiya Segodnya, especially that of its subordinate online news outlet Sputnik. The pages represented a systematic, covert attempt to improve Rossiya Segodnya's online audience across more than a dozen countries. […] Sputnik was the main beneficiary, as it was often the only source the Facebook pages amplified." READ MORE

RELATED ARTICLES

Facebook, Removing Coordinated Inauthentic Behavior from Russia, 17 Jan 2019

Source: ABC

Date: 31 Jan 2019

Tonga's internet outage and Pacific's vulnerability

"Tonga is on the verge of having its internet access restored, more than ten days after its undersea fibre optic cable was severed. The cable was broken in at least two places by, what the company says, was the anchor of a ship operating in an area that is supposed to be off-limits. Submarine cable breakages are relatively common, but experts say Pacific countries are especially vulnerable because they are reliant on so few cables to connect them to the rest of the world." READ MORE

Source: DevPolicy Blogs

Date: 21 Jan 2019

Controlling the internet in Fiji

"In late 2017 the Fijian Government and its key officials called for the regulation of Fiji's cyber space. By May 2018, Fiji's Parliament had passed the Online Safety Act, which was publicised as a law designed to protect Fijians against harmful online behavior, such as cyber stalking, cyber bullying, revenge porn and internet trolling. The Act came into effect on 1 January this year, and in late December the Government announced the appointment of a Commissioner to administer it. Fiji's tumultuous political history has put immense pressure on its media freedom and landscape. Given this, blogs and social media have played the important role of providing Fijians with greater access to uncensored information. On the other hand, greater internet and online access has also brought an onslaught of cyber-related crimes and issues. As such, the Act must maintain a balance between not undermining free speech, while still providing safeguards against malicious online behavior." READ MORE

Source: IT Web Africa

Date: 28 Jan 2019

Kenya should expect more cyber-attacks

"According to Kaspersky Lab Africa, 33.5% of internet users in Kenya faced internet borne cyber threats in 2018, with an estimated 20 million-plus attacks throughout the period." If we compare with 2017, we see that there was an increase in the number web-borne threats, almost four times," said Robert Badenhorst, Managing Director. Statistics from the Communication Authority of Kenya (CA) support Kaspersky's findings. […] The National Cybersecurity Centre reported 6,384 cyber threat cases that were escalated compared to 2,613 in the previous quarter. […] The CA report reflected an increase in online impersonation which is often used in engineering an attack. In the third quarter 2018, there were 196 reported cases of online impersonation compared to 34 cases in the previous quarter." READ MORE

Source: ITWeb Africa

Date: 31 Jan 2019

Zimbabwe fast-tracks cybercrime legislation

"Following two years of consideration, Zimbabwe's cabinet has approved the Cybercrime and Cyber Security Bill. […] The Cybercrime and Cyber Security Bill was reportedly fast-tracked by Zimbabwe's Information Minister last week following widespread protest action over price hikes on fuel and other commodities, which made international headlines. In response the government shut down the internet and social media access citing the Interception of Communications Act. According to the newly introduced laws, Zimbabweans who abuse social media will face maximum ten years in jail, and foreign-based Zimbabweans "who cause harm back home" using social media or any other computer-based system will be extradited and prosecuted. […] Thabani Moyo, director of Media institute of South Africa, said, "If the bill takes effect, it will give the state authorities enormous power to obtain information freely on any individual, including accessing, making copies and collecting individual information or even entering the house of a person with no court warrant."" READ MORE

Source: Safety Detective

Date: 15 Jan 2019

Major Security Breach Discovered Affecting Nearly Half of All Airline Travelers Worldwide

"Hacker and Activist Noam Rotem, working with Safety Detective research lab, was shocked when he recently discovered a major vulnerability affecting nearly half of all airlines worldwide. While booking a flight with Israeli national carrier ELAL, he came across a significant security breach that allows anyone to access and change private information on flight bookings. The same breach was then discovered to include 44% of the international carriers market, potentially affecting tens of millions of travelers. According to ELAL, the bug stems from their supplier Amadeus' online booking system, which controls a staggering 44% market share of airlines operating worldwide, including United Airlines, Lufthansa, Air Canada, and many more." READ MORE

Source: ANADOLU AGENCY

Date: 17 Jan 2019

10 FETO suspects detained in Izmir over ByLock use

Turkish police have detained 10 people with suspected links to the Fetullah Terrorist Organization (FETO) in the Aegean province of Izmir, security sources said Thursday. The detentions came from arrest warrants issued by Izmir prosecutors for 12 suspects with various backgrounds, said the sources, who asked not to be named due to restrictions on speaking to the media. A search for the remaining two suspects continues. The suspects are accused of using ByLock, an encrypted cellphone app said to be used by FETO members to communicate during and after the defeated 2016 coup. READ MORE

RELATED ARTICLES

Stockholm Center for Freedom, Turkey orders detention of 222 people over Gülen links in one day, 15 Jan 2019

Source: Mind Media

Date: 31 Jan 2019

"Le Cloud Act américain est-il compatible avec le RGPD européen ?"

[…] En substance, le Cloud Act ne créé pas un nouveau régime d'accès aux données, mais vient préciser le cadre existant. Le Cloud Act modifie ainsi le Stored Communications Act (SCA) un chapitre du United States Code (U.S.C) équivalent aux codes pénal et de procédure pénale français. Il est important de souligner que le régime d’accès aux données prévu par le SCA ne prévoit pas un droit qui serait absolu et illimité. Une première limite tient aux types d’opérateurs et de données concernés. Le SCA vise uniquement les fournisseurs de services de communications électroniques (ECS) - par exemple des opérateurs téléphoniques ou des FAI (voire un site web qui offrirait à ses clients la possibilité d'envoyer des messages ou des communications à des tiers), et les fournisseurs de services informatiques à distance (RCS) - par exemple un fournisseur de services d’hébergement dans le Cloud. Une entreprise qui n’entre pas dans ces catégories d’opérateurs ne peut être directement visée par une demande fondée sur le Cloud Act. READ MORE

Latest reports

- ENISA, Training course material on network forensics for cybersecurity specialists, 28 Jan 2019
- SBS News, How 10 years of cyber-racism has transformed society, 31 Jan 2019
- We Live Security, Cybercrime black markets: Dark web services and their prices, 31 Jan 2019
- Cyber Risk Management (CyRiM) project, Bashe attack - Assessing the impact of a global ransomware attack, 29 Jan 2019
- MalwareBytes, 2019 State of Malware, January 2019
- FireEye, APT39: An Iranian Cyber Espionage Group Focused on Personal Information, 29 Jan 2019
- ASPI - The Strategist, Hackers for hire pose growing international security risk, 24 Jan 2019

Upcoming events

- 4 – 8 February, Tunis, Tunisia – Advanced judicial training, CyberSouth
- 11 – 15 February, Bucharest, Romania – ECTEG regional training on Network Investigations in cooperation with the Romanian Police Academy, iPROCEEDS
- 11 – 15 February, San José, Costa Rica – Introductory Judicial Training of Trainers (ToT) on cybercrime and electronic evidence for magistrates and prosecutors, GLACY+
- 11 – 15 February, Rabat, Morocco – ECTEG training: Internet Investigation and Darknets, delivered by INTERPOL, GLACY+
- 14 – 15 February, Santo Domingo, Dominican Republic – Advisory mission on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence, GLACY+
- 15 February, Bucharest, Romania – Awareness raising meeting on the Budapest Convention, benefits and challenges for Embassies of priority countries, 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

COUNCIL OF EUROPE

CONSEIL DE L’EUROPE

www.coe.int/cybercrime