Cybercrime Digest

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

15-28 February 2019

Source: Council of Europe

Date: 28 Feb 2019

Criminal Justice in Cyberspace: key messages

"While cyber threats and their impact are increasing and touching upon core values of societies in Europe and worldwide, criminal justice authorities are faced with complex challenges. At the same time, solutions are in place or are being developed. Examples are the E-evidence proposals at the European Union or the preparation of an additional Protocol to the Budapest Convention on Cybercrime at the Council of Europe. And both organisations have been supporting capacity building on cybercrime worldwide for many years. Under the Romanian Presidency of the Council of the European Union, a conference on "*Criminal Justice in Cyberspace*" has been organised by the Ministry of Justice of Romania in cooperation with the Council of Europe, on 25 - 27 February 2019, in Bucharest, Romania. The purpose of the conference was to add further momentum to solutions in place or in preparation and to promote cooperation at all levels to strengthen the rule of law in cyberspace. The event was aimed at cybercrime experts from the European Union Member States, Eastern Partnership countries, parties to the Budapest Convention and service providers. Key messages of the conference can be accessed here." CONFERENCE WEBSITE

RELATED ARTICLES

Gabriella Battaini-Dragoni, Deputy Secretary General of the Council of Europe, Welcome Remarks, 26 Feb 2019

Source: ENISA

Date: 28 Feb 2019

ENISA makes recommendations on EU-wide election cybersecurity

"Through this paper, ENISA puts forward a set of recommendations aimed at improving the cybersecurity of elections across the EU and supporting the Member States in their efforts. The most important recommendations that ENISA makes are: Member States should consider introducing national legislation to tackle the challenges associated with online disinformation while protecting to the maximum extent possible the fundamental rights of EU citizens; Member States should continue to actively work together with the aim to identify and take down botnets; Consideration should be given to regulation of Digital Service Providers, social media, online platforms and messaging service providers at an EU level to ensure a harmonised approach across the EU to tackling online disinformation aimed at undermining the democratic process; The above players are also advised to deploy technology that will identify unusual traffic patterns that could be associated with the spread of disinformation or cyberattacks on election processes; A legal obligation should be considered to classify election systems, processes and infrastructures as critical infrastructure so that the necessary cybersecurity measures are put in place; A legal obligation should be put in place requiring political organisations to deploy a high level of cybersecurity in their systems, processes and infrastructures; Official channels/technologies for the dissemination of the results should be identified, as well as back-up channels/technologies that validate the results with the count centres. Where websites are being used, DDoS mitigation techniques should be in place." READ MORE

Source: Reuters

Date:20 Feb 2019

Microsoft says discovers hacking targeting democratic institutions in Europe

"The hacks occurred between September and December 2018, targeting employees of the German Council on Foreign Relations and European offices of The Aspen Institute and The German Marshall Fund, the company said here in a blog post. Microsoft said it discovered the hacking through the company's Threat Intelligence Center and Digital Crimes Unit, and the hacks targeted 104 employee accounts in Belgium, France, Germany, Poland, Romania, and Serbia. Hackers in most cases create malicious weblinks and spoofed email addresses that look legitimate, aiming to gain access to employee credentials and deliver malware, the company said." READ MORE

RELATED ARTICLES

Motherboard, Experts Find Serious Problems With Switzerland's Online Voting System Before Public Penetration Test Even Begins, 21 Feb 2019

Reuters, Ukraine security service accuses Russia of meddling in election, 21 Feb 2019

Source: World Economic Forum

Date:19 Feb 2019

Fighting cybercrime – what happens to the law when the law cannot be enforced?

"The widespread loss of trust in the internet is the fifth greatest strategic risk facing the world, according to the World Economic Forum's Global Risks Report 2019. […] Cybercrime will continue to be the security challenge of the 21st century. In the context of cyber security as a major global risk, the global community needs to recognize that there is a "stunning enforcement gap", as a recent report by the Third Way highlights. Not only is the current wave of cybercrime largely unseen, but the chances of being successfully investigated and prosecuted for a cyber attack in the US are now estimated at 0.05%. This mirrors similar reports from around the world. This is for a crime type that is predicted to be costing the global economy $6 trillion by 2021. For violent crime, the equivalent chance is 46%. The global community needs to ask itself why this is happening, and what can be done to change it." READ MORE

Source: U.S. Department of Justice

Date: 25 Feb 2019

U.S. Deputy Attorney General delivers remarks on defending rule of law norms

"[…] Some countries seek to advance their ends by changing global criminal justice norms. For instance, Russia and China seek to replace the Budapest Convention on Cybercrime. That Convention is approved by the United States and more than 60 other nations. It harmonizes national interests and enhances the flow of electronic evidence among nations to facilitate the investigation of cybercrimes — while balancing civil liberties and privacy interests. Russia rejects the Budapest Convention, complaining that the pact allows individual owners of data to control it. In its place, Russia seeks to advance a new convention that would enhance the ability of regimes to control communication, limit information-sharing between nations, and impede efforts to investigate cybercrime. We reject the effort to undermine the goal of an open Internet governed by the rule of law and protected by international cooperation. I want to emphasize that the people of China, Russia, and other nations that do not share our respect for individual rights are not our enemies." READ MORE

Source: Ghana Web

Date:21 Feb 2019

Government of Ghana step up nationwide cyber security efforts

"According to recent research, the activities of cybercriminals have had a devastating impact on Ghana's economy in the past couple of years. The Cybercrime Unit within the Ghana Police Services has released details of how cybercrime has cost the country roughly $230 million in the period from 2016 to August 2018. […] Against this landscape, the government has decided to take measures to play their part in increasing our vigilance and the capacity for an institutional response against cybercriminals. […] Implementing its longstanding goal of digital safety, the Ministry has established an administrative hub that will coordinate cybersecurity efforts across the public and the private sectors, the National Cyber Security Centre. […] It has also managed to accede to two seminal international cybersecurity instruments, the Budapest Convention against Cybercrime and the Malabo Convention on Cyber Security and Personal Data Protection. Recently, Ms. Owusu-Ekuful, the Communications Minister, has announced that the Ministry is also currently developing a law that will serve to improve Ghana's cybersecurity landscape as a whole." READ MORE

Source: ICANN

Date:22 Feb 2019

ICANN: There is an ongoing and significant risk to DNS infrastructure

"The Internet Corporation for Assigned Names and Numbers (ICANN) believes that there is an ongoing and significant risk to key parts of the Domain Name System (DNS) infrastructure. In the context of increasing reports of malicious activity targeting the DNS infrastructure, ICANN is calling for full deployment of the Domain Name System Security Extensions (DNSSEC) across all unsecured domain names. […] On 15 February 2019, in response to reports of attacks against key parts of the DNS infrastructure, ICANN offered a checklist of recommended security precautions for members of the domain name industry." READ MORE

RELATED ARTICLES

Krebs on Security, A Deep Dive on the Recent DNS Hijacking Attacks, 18 Feb 2019

Source: Kathmandu Post

Date:21 Feb 2019

Nepal, 'Information Technology Regulation Act' tabled in Parliament

"The Nepal government recently tabled 'Information Technology Regulation Act' in Parliament. This bill aims to replace two existing technology laws: The Electronics Transaction Act 2063 and the National Technology Development Board Order 2058. […] The preamble of the bill states its main objectives: Regulate the Information Technology industry; Regulate electronic records and signatures; Provide public service through information technology; Ensure cybersecurity; protect users' data, control cybercrime, regulate domain names, social media, among others. The bill envisions three different institutional mechanisms: A National Information Technology Center, an Information Technology Court and an Office of The Controller on Digital Signatures. […] The bill defines 'crime and offense' through the Information Technology medium and also proposes a procedural approach for tech-related investigations and judicious processes. […] The bill, after being tabled in Parliament,

has been received controversially for its ambiguous regulations on social media." READ MORE

Source: Economia Hoy

Date:26 Feb 2019

Empresas llaman a cambiar el paradigma de seguridad cibernética en México

"Con un panel conformado con expertos en diferentes rubros de ciberseguridad, se realizó el primer Seminario de Ciberseguridad Financiera, que analizó los recientes ataques contra entidades financieras y posibles soluciones a futuro. […] Sobre el marco jurídico actual para castigar a los ciberdelincuentes, Andrés Velázquez, especialista en Seguridad Informática, explicó que la legislación actual sí tiene mecanismos de protección, más no los adecuados. Refirió que México no está adherido al Convenio de Budapest, lo que obstaculiza la cooperación internacional y extradición por delitos financieros, además de que ayudaría la tipificación de delitos y aumento en sentencias condenatorias." READ MORE

Source: Cape Town Etc

Date:18 Feb 2019

South Africa, new Cybercrime Bill up for comment

"The public is encouraged to submit their comments on the arriving Cybercrimes Bill, which was passed by the National Assembly in November 2018. This version, however, is quite different from those previously published. The old bill was divided into two parts, cybercrime and cybersecurity respectively. While the cybercrimes section was praised, the proposed cybersecurity security section raised concerns on how this would affect the government's censoring of the freedom of speech of individuals, as well as their rights. Having taken this into consideration, the Portfolio Committee on Justice and Correctional Services decided to abolish all clauses pertaining to cybersecurity, and only focus on cybercrimes." READ MORE

Source: The Diplomat

Date:20 Feb 2019

The Cyber War Against Tibet

"A group of world-class researchers, analysts, and engineers, recently uncovered a new cyberespionage campaign delivering a malicious Microsoft PowerPoint document using a mailing list run by the Central Tibetan Administration (CTA). The document is a copy of a legitimate PDF file titled "Tibet was never a part of China," which is available for download from the CTA's website tibet.net. The malicious version, however, contains a Remote Access Trojan (RAT). The email is targeted at pro-Tibet groups and individuals in order to distribute what has been dubbed ExileRAT. The attack delivers an Android- and Windows-based Trojan capable of stealing system and personal information, terminating or launching process, or carrying out surveillance and the theft of data. […] The Tibetan community has been persistently targeted by digital espionage operations for over a decade." READ MORE

Source: Cyber Scoop

Date:21 Feb 2019

Blind Eagle, a new APT group, poses as Colombia's Cyber Police to steal business secrets

"A new hacking group researchers have dubbed Blind Eagle is carrying out targeted attacks against Colombian government agencies, financial companies and corporations with a presence in Colombia. Blind Eagle has been active since April 2018, posing as Colombian institutions like the National Cyber Police and the Office of the Attorney General to steal intellectual property, according to research published this week by the

360 Enterprise Security Group. […] Researchers suggested the attacks originated in South America, based on the timing and the use of Spanish language" READ MORE

Source: Access Now

Date:19 Feb 2019

Cybercrime law in Jordan: pushing back on new amendments that could harm free expression and violate privacy

"In recent months, Amman has witnessed widespread protests and a popular rejection of an amended cybercrime bill that contains provisions that restrict freedom of expression online and the right to privacy. […] On February 19, 2019, the Jordanian Parliament discussed the cybercrime bill at its 22nd session. The session concluded with a majority voted in favor of MP Abdelkrim Daghmi's proposal to refer the bill to the Jordanian government for the purpose of introducing necessary amendments to some articles, especially those related to hate speech and fake news. […] The most recent amendments introduce an ambiguous definition of "hate speech," defined as "every writing and every speech or action intended to provoke sectarian or racial sedition, advocate violence or foster conflict between followers of different religions and various components of the nation." […] Moreover, the amended text would serve to smudge the line between hate speech and legitimate criticism of public figures on social media. […] These provisions could easily be used to target activists and human rights defenders." READ MORE

Latest reports

- European Parliament, The new European cybersecurity competence centre and network, February 2019
- Corte Suprema de Chile, Informe sobre proyecto de ley de delitos informáticos, 12 Feb 2019
- Google Europe, Fighting disinformation across our products, 16 Feb 2019
- The Asan Institute for Policy Studies, The Evolution of North Korean Cyber Threats, 20 Feb 2019
- HelpNet Security, Social media-enabled cybercrime is generating $3.25 billion a year, 27 Feb 2019
- IBM, X-Force Report: Ransomware Doesn't Pay in 2018 as Cybercriminals Turn to Cryptojacking for Profit, 26 Feb 2019
- Sapienza University of Rome, Peel the onion: Recognition of Android apps behind the Tor Network, February 2019

Upcoming events

- 2-3 March, Colombo, Sri Lanka – Workshop on cybercrime for the intake of new judges, GLACY+
- 3-7 March, Algiers, Algeria – Working group on the integration of the cybercrime judicial training, CyberSouth
- 4-7 March, Tirana, Albania – Case simulation exercise on cybercrime and financial investigations (Albania and Kosovo*), iPROCEEDS
- 4-8 March, Bucharest, Romania – Training on Darkweb and cryptocurrency, CyberSouth
- 5 March, Brussels, Belgium – Coordination Meeting with EU-funded Cybercrime projects (OCWAR-C, GLACY+, CIBER4Dev), GLACY+
- 11-12 March, Abidjan, Côte d'Ivoire – Awareness raising workshop on the Budapest Convention, Cybercrime@Octopus
- 11-12 March, Podgorica, Montenegro – Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (1st part), iPROCEEDS

- 11-12 March, Belgrade, Serbia - Advice to public authorities and law reform working group to bring legal framework in line with EU and Council of Europe standards (assessment of legislation: advisory mission and desk review), iPROCEEDS
- 11-13 March, Bucharest, Romania - Kick-off meeting of EMPACT OAP 2019 - update of the ECTEG Dark Web and Virtual Currencies Training in cooperation with SELEC, iPROCEEDS / GLACY+ / Cybercrime@Octopus
- 11-15 March, Santo Domingo, Dominican Republic – Advanced Judicial Training on cybercrime and electronic evidence for judges, magistrates and prosecutors, GLACY+

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