Cybercrime Digest

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

1 – 15 February 2021

Source: Council of Europe

Date: 15-25 Feb 2021

INTERPOL & GLACY+ webinaires techniques : Crypto pour les autorités de justice pénale

"Le 15 février INTERPOL et le projet GLACY+ ont lancé la série de cinq webinaires techniques en Français pour les fonctionnaires de justice pénale. Destinées en particulier aux agents de police, procureurs, juges et autres professionnels, les sessions sont conçues de telle manière qu'elles permettent aux participants se doter de connaissances techniques en cryptographie. Les ateliers répondent à un réel besoin de formation constaté les dernières années et visent à fournir une compréhension conceptuelle de la cryptographie, si nécessaire pour l'enquête efficace des infractions informatiques." READ MORE

Source: ABC Pacific Beat

Date: 15 Feb 2021

Fiji passes new cybercrime laws

"Fiji's parliament has passed new laws that aim to crack down on people committing cybercrimes […] Fiji's Attorney General Aiyaz Sayed-Khaiyum said they provide a comprehensive and coherent framework on cybercrime and electronic evidence. Jope Tarai an assistant lecturer in Ethics and Governance at the University of the South Pacific says Fiji will need assistance when it comes to increasing authorities' capability to investigate crimes that happen online and collect digital evidence. "Capacity is always going to be a challenge and that's where the cooperation with other states becomes crucial, with Australia, New Zealand and various other partners, because they transcend boundaries especially when it comes to financial fraudulent activities," he told Pacific Beat." READ MORE

RELATED ARTICLES

Parliament of the Republic of Fiji, Standing Committee on Justice, Law and Human Rights, Review Report on the Cybercrime Bill 2020, (Bill No. 11 of 2020), Feb 2021

FBC, Cybercrime Bill to boost investor confidence, 12 Feb 2021

Source: Ecuardorenvivo.com

Date: 20 Jan 2021

Ecuador: Expertos proponen tipificar el delito de acoso digital de manera urgente

"En el marco de la discusión y socialización del Proyecto de Ley Orgánica para Prevenir la Violencia, el Acoso Digital y la Violación a la Intimidad, la Comisión de Justicia, en la sesión 144, escuchó los puntos de vista de los expertos Santiago Martín Acurio del Pino y Gabriel Llumiquinga, quienes coincidieron en la necesidad de tipificar el ciberacoso, más aún cuando afecta a grupos vulnerables como niñas, adolescentes y mujeres. Los especialistas exhortaron, a la brevedad posible, que Ecuador proceda a suscribir el Convenio de Budapest contra el Cibercrimen, de la Unión Europea, que constituye el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet, mediante la armonización de leyes entre naciones, para la mejora de las técnicas de investigación, la prevención y sanción." READ MORE

Source: AP News

Date: 10 Feb 2021

UN experts: North Korea using cyber attacks to update nukes

"North Korea has modernized its nuclear weapons and ballistic missiles by flaunting United Nations sanctions, using cyberattacks to help finance its programs and continuing to seek material and technology overseas for its arsenal including in Iran, U.N. experts said. The panel of experts monitoring sanctions on the Northeast Asian nation said in a report sent to Security Council members Monday that North Korea's "total theft of virtual assets from 2019 to November 2020 is valued at approximately $316.4 million," according to one unidentified country. The panel said its investigations found that North Korean-linked cyber actors continued to conduct operations in 2020 against financial institutions and virtual currency exchange houses to generate money to support its weapons of mass destruction and ballistic missile programs." READ MORE

Source: Washington Post

Date: 2 Feb 2021

Russia is trying to set the rules for the Internet. The U.N. saw through the ruse

"Russia is engaged in a brazen but little noticed effort to set new rules for cyberspace — even as it flouts the existing ones. Last week, in an encouraging step, a United Nations telecommunications body pushed back. Russia had asked the International Telecommunications Union (ITU) to have the group's 193 member states "discuss the status of global governance system for … Internet domain names, addresses, and critical Internet infrastructure." In a curt statement Thursday, the ITU said simply that it had "noted the contribution" of Russia. […] One European delegate to the conference said the opaque official language meant that no further action would be taken. He noted that the Russians tried again by attaching a similar proposal to an ITU measure involving protection of children online, but it was also rejected. The ITU operates by consensus, so opposition from the United States and key European and Asian allies was enough to scuttle the Russian moves." READ MORE

Source: Council of Europe

Date: 9 Feb 2021

Workshop on the preparation of cybercrime and e-evidence situation report in Jordan

"The workshop was an opportunity for the Jordanian authorities to express their views on the cybercrime situation in the country, by emphasizing the legal and technical tools for conducting investigations and collecting e-evidence, as well as the developments on the cybercrime policies and strategies. The experts underlined the importance of having a National Cyber Security Strategy with mechanisms to tackle cybercrime. The relevance of the annual situation report on cyber threats was discussed in depth and recommendations were put forward in relation to its structure and contributors. Furthermore, the importance of communication at the strategical and operational levels, multi-disciplinary approach towards addressing cybercrime, the benefits of reporting, as well as the need of the statistics and reporting were touched upon." READ MORE

RELATED ARTICLES

Council of Europe, Workshop on the preparation of cybercrime and e-evidence situation report in Morocco, 3 Feb 2021

Source: The Economist

Date: 13 Feb 2021

Censorious governments are abusing "fake news" laws

"During his final days Mohamed Monir, an Egyptian journalist, was so short of breath he could barely speak. In a video recorded in July last year, as his final hours approached, he begged for oxygen. He died in a hospital isolation unit after contracting covid-19 in prison while awaiting trial. He had been arrested the previous month after, among other things, writing an article lambasting the Egyptian government's response to the pandemic. He was charged with spreading false news, misusing social media and joining a terrorist group. Covid-19 has indeed unleashed a flood of misinformation. But it has also given governments such as Egypt's an excuse to crack down on their critics using the pretext of restricting the spread of fake news. Between March and October last year 17 countries passed new laws against "online misinformation" or "fake information", according to the International Press Institute" READ MORE

Source: Axios

Date: 2 Feb 2021

Internet blackouts skyrocket amid global political unrest

"At least 35 countries have restricted access to the internet or social media platforms at least once since 2019, according to NetBlocks, a group that tracks internet freedom. Authorities have used the outages to reduce or prevent unrest — or to hide it from public view. Blockages are particularly common around elections in Africa, most recently in Uganda. NetBlocks also reported disruptions in Russian cities during recent protests over the detention of Alexei Navalny. Neighboring Belarus also disrupted the internet during recent protests, as have countries from Algeria to Zimbabwe." READ MORE

Source: The Verge

Date: 8 Feb 2021

Hackers tampered with a water treatment facility in Florida by changing chemical levels

"Hackers successfully infiltrated the computer system controlling a water treatment facility in the city of Oldsmar, Florida, according to a report from the *Tampa Bay Times*. In doing so, the hackers were able to remotely control a computer to change the chemical levels of the water supply, increasing the amount of sodium hydroxide before a supervisor was able to catch the act in real time and revert the changes. "At no time was there a significant adverse effect on the water being treated," Pinellas County Sheriff Bob Gualtieri said during a press conference on Monday, later posted to YouTube. "Importantly, the public was never in danger." READ MORE

Source: ZD Net

Date: 8 Feb 2021

Hacktivists deface multiple Sri Lankan domains, including Google.lk

"A mysterious group of hacktivists has poisoned the DNS records of several Sri Lankans (.lk) websites on Saturday and redirected users to a web page detailing various social issues impacting the local population. While most of the affected domains were websites for local businesses and news sites, two high-profile domains for Google.lk and Oracle.lk, were also impacted, readers told *ZDNet* on Saturday. A message was displayed on Google.lk for a few hours before authorities intervened. The message highlights issues with the local tea-growing industry, freedom of the press, the alleged corrupt political class and judicial system, and racial, minority, and religious issues." READ MORE

Source: Reuters

Date: 14 Feb 2021

Myanmar's proposed cybersecurity Bill draws wide condemnation

"A group of the world's biggest internet companies joined Myanmar civil society on Thursday in raising alarm over cyber laws floated by the new junta, saying they would contravene fundamental rights and hurt the economy. The 36 pages outlining the proposed laws were given to mobile operators and telecoms license holders for comment on Tuesday - just over a week after the army overthrew the elected government of Aung San Suu Kyi, the civil society groups said. The proposed bill would give unprecedented censorship powers and violate privacy, contravening democratic norms and fundamental rights, said the Asia Internet Coalition, whose members include Apple, Facebook, Google and Amazon. "This would significantly undermine freedom of expression and represents a regressive step after years of progress," the group said in a statement." READ MORE

Source: Council of Europe

Date: 5 Feb 2021

Work in progress on SOPs and Toolkit for first responders on cybercrime and electronic evidence in Morocco

"Under the framework of the CyberSouth Project, on the 5th of February 2021, the Second online national meeting on the development of a domestic Standard Operating Procedures (SOPs) and Toolkit for First Responders in Cybercrime Investigations and E-evidence, was held with Morocco, for the benefit of the law enforcement representatives dealing with cybercrime and e-evidence. The purpose of this meeting was to follow-up with the members of the working group established after the first workshop on SOPs, which took place on the 22nd of September 2020. The goal of the present online meeting was to discuss with the Moroccan representatives the draft Guide on the Identification, Collection, Preservation and Analysis of Digital Evidence, its content and structure. The activity had an interactive approach, with the Moroccan working group liaising with the Council of Europe's representative, consultant and Interpol, on the structure and aim of the draft guide. Moreover, the gaps, and concrete recommendations on how to align it with the national legislation, international best practices and the actual investigation techniques applied in Morocco, were also brought up." READ MORE

Source: The Hacker News

Date: 9 Feb 2021

Ukrainian Police Arrest Author of World's Largest Phishing Service U-Admin

"Law enforcement officials in Ukraine, in coordination with authorities from the U.S. and Australia, last week shut down one of the world's largest phishing services that were used to attack financial institutions in 11 countries, causing tens of millions of dollars in losses. The Ukrainian attorney general's office said it worked with the National Police and its Main Investigation Department to identify a 39-year-old man from the Ternopil region who developed a phishing package and a special administrative panel for the service, which were then aimed at several banks located in Australia, Spain, the U.S., Italy, Chile, the Netherlands, Mexico, France, Switzerland, Germany, and the U.K. Computer equipment, mobile phones, and hard drives were seized as part of five authorized searches conducted during the course of the operation. Security researcher Brian Krebs noted the raids were in connection with U-Admin, a phishing framework that makes use of fake web pages to pilfer victim credentials more efficiently." READ MORE

Source: ZD Net

Date:14 Feb 2021

Egregor ransomware operators arrested in Ukraine

"Members of the Egregor ransomware cartel have been arrested this week in Ukraine, French radio station France Inter reported on Friday, citing law enforcement sources. The arrests, which have not been formally announced, are the result of a joint investigation between French and Ukrainian police. […] The Egregor gang, which began operating in September 2020, operates based on a Ransomware-as-a-Service (RaaS) model. They rent access to the actual ransomware strain, but they rely on other cybercrime gangs to orchestrate intrusions into corporate networks and deploy the file-encrypting ransomware. Victims who resist paying the extortion fee are often listed on a so-called "leak site," in the hopes of shaming them into paying the ransom demand. Victims who don't pay often have internal documents and files shared on the Egregor leak site as punishment." READ MORE

RELATED ARTICLES

France Inter, Cybersécurité : des pirates "Egregor", à l'origine de l'attaque contre Ouest-France, interpellés en Ukraine, 12 Feb 2021

Source: Council of Europe

Date: 20 Jan 2021

Republic of Moldova: Webinar on online child sexual abuse for police, judges and prosecutors

"On 11 February 2021 the Council of Europe regional project End Online Child Sexual Exploitation and Abuse @ Europe (EndOCSEA@Europe) and project on Combating violence against children in the Republic of Moldova held the "Introductory session on online child sexual abuse and exploitation (OCSEA)", a webinar for police, judges and prosecutors, designed to enhance criminal justice capacities and increase interagency cooperation. It offered a set of information related to standards on OCSEA, focusing on relevant Lanzarote Convention articles relating to the removal of the alleged perpetrator and support and assistance during and after investigation and criminal proceedings to OCSEA and the protection of child victims and witnesses in criminal proceedings. It also looked at the relevant Budapest Convention articles covering elements such as production order and search and seizure of stored computer data." READ MORE

Source: World Economic Forum

Date: 12 Feb 2021

Fifth-generation cyberattacks are here. How can the IT industry adapt?

"Cyberattacks have reached a new level of sophistication, ranging from international espionage to massive breaches of personal information to large-scale internet disruption. Advanced "weapons-grade" hacking tools have been leaked, allowing attackers to move fast and infect large numbers of businesses and entities across huge swaths of geographic regions. Large-scale, multi-vector mega-attacks have sparked a need for integrated and unified security structures. Most businesses are still in the world of second- or third-generation security, which only protects against viruses, application attacks and payload delivery. Networks, virtualized data centres, cloud environments and mobile devices are all left exposed. To ensure a cybersecure organization, businesses must evolve to fifth-generation security: advanced threat prevention that uniformly prevents attacks on a business's entire IT infrastructure." READ MORE

Source: Europol

Date: 10 Jan 2021

Ten hackers arrested for string of sim-swapping attacks against celebrities

“A total of 8 criminals have been arrested on 9 February as a result of an international investigation into a series of sim swapping attacks targeting high-profile victims in the United States. These arrests follow earlier ones in Malta (1) and Belgium (1) of other members belonging to the same criminal network. The attacks orchestrated by this criminal gang targeted thousands of victims throughout 2020, including famous internet influencers, sport stars, musicians and their families. The criminals are believed to have stolen from them over USD 100 million in cryptocurrencies after illegally gaining access to their phones. This international sweep follows a year-long investigation jointly conducted by law enforcement authorities from the United Kingdom, United States, Belgium, Malta and Canada, with international activity coordinated by Europol.” READ MORE

Latest reports

- European Data Protection Board, Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), 2 February 2021
- Council of the European Union, Cybersecurity: how the EU tackles cyber threats, 12 February 2021
- ENISA, Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving, 11 February 2021
- ENISA, Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies, 9 February 2021
- ENISA, Solving the Cryptography Riddle: Post-quantum Computing & Crypto-assets Blockchain Puzzles, 9 February 2021
- Ministerio Público Fiscalía de la Nación Peru, Guía Práctica para solicitar la Prueba Electrónica a través de las fronteras, 12 February 2021
- Chatham House, The SolarWinds Hack: A Valuable Lesson for Cybersecurity, 2 Feb 2021
- Chainalysis, Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think, 26 Jan 2021
- Bloomberg Law, To Pay or Not to Pay: Ransomware Threats and Risking Payment Sanctions, 4 February 2021
- ESET, ESET Threat Report Q42020, 10 Feb 2021
- SecureList, DDoS attacks in Q4 2020, 16 Feb 2021

Upcoming events

- 15, 17, 22, 24 & 25 February, C-PROC/INTERPOL (on-line), Series of GLACY+ & INTERPOL webinars on Encryption (FR), GLACY+
- 15-16 February, C-PROC/Moldova, (on-line), Workshop with personal data protection authorities and national communications regulators on trust and cooperation, CyberEast
- 17 February, C-PROC/Algeria, (on-line), Workshop on the preparation of the national cybercrime and e-evidence situation report, CyberSouth
- 18 February, C-PROC/Algeria (on-line), Workshop on the development of the SOPs on e-evidence, CyberSouth
- 22-24 February, C-PROC/Azerbaijan, (on-line), Training on international cooperation on cybercrime and electronic evidence for investigators, prosecutors and judges, CyberEast
- 22, 23 & 24 February, C-PROC/Strasbourg, (on-line), T-CY: Protocol Drafting Group meeting - T-CY, Octopus Project
- 22-23 February, C-PROC/Morocco, (on-line), 3rd meeting of the national working group on the finalization of the judicial training material, CyberSouth
- 23-25 February, C-PROC/Turkey, (on-line), Online training course for the candidate magistrates on countering online child sexual exploitation, iPROCEEDS-2, EndOCSEA@Europe
- 24 February, C-PROC, (on-line), Series of monthly thematic webinars for the International Network of the National Judicial Trainers, GLACY+
- 25 February, C-PROC, (on-line), Regional Workshop on interagency cooperation on the search, seizure and confiscation of on-line crime proceeds, CyberSouth
- 25 February, C-PROC/Georgia, (on-line), Workshop with Georgian authorities on the reform of criminal procedure legislation, CyberEast
- 26 February, C-PROC, (on-line), Webinar on Hate Speech and Restrictive Measures: cyberviolence series, CyberEast
- 26 February, C-PROC/Strasbourg, (on-line), T-CY: Protocol Drafting Plenary - T-CY, Octopus Project
- By 28 February, C-PROC, Preparation of country profiles on online child sexual exploitation and abuse, Octopus Project, EndOCSEA@Europe
- By 28 February, C-PROC, Desk review of the national legislation on cybercrime and electronic evidence in the Caribbean region, Octopus Project in cooperation with CARICOM IMPACS

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of February have been rescheduled to a later date.

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