Cybercrime Digest

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

15 – 31 March 2022

Source: Agence Europe

Date: 29 Mar 2022

Commission proposes negotiating mandate for future UN Convention against Cybercrime

"The European Commission proposed, on Tuesday 29 March, a negotiating mandate for the EU to take part in the negotiations on a new international convention to combat the use of information and communication technologies for criminal purposes. The negotiations, which began in early 2022 and are expected to end in 2024, follow a December 2019 UN resolution on combating the criminal use of these technologies." READ MORE

RELATED DOCUMENT:

EUR-LEX, Recommendation for a COUNCIL DECISION authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, 29 Mar 2022

Source: Global Initiative

Date: 17 Mar 2022

Cyber, fire and fury

"Overshadowed by Russia's invasion of Ukraine – and with relations between the West and Russia at a low point – member states did nevertheless manage to achieve consensus on the negotiation's processes, but major differences on policy remain unresolved. […] There were some areas of relative agreement. There was also broad support, at least in principle, for the involvement of civil society, NGOs, academia and the private sector in understanding and developing best practices to combat cybercrime." READ MORE

Source: Council of Europe

Date: 30 Mar 2022

The Government of Italy makes a voluntary contribution to the Octopus Project

"The Government of Italy has made a voluntary contribution of EUR 10 000 to the Council of Europe action on cybercrime through the Octopus Project, in particular for the international conference dedicated to the Opening for signature of the Second Additional Protocol to the Convention on Cybercrime, to take place in Strasbourg between 12-13 May 2022." READ MORE

Source: Eurojust

Date: 31 Mar 2022

Takedown of online investment fraud in Albania: 15 arrests

"With support from Eurojust, authorities in Albania and Germany have taken down a fraudulent online investment platform that defrauded victims, including many Germans, of at least several million euros. During a recent action day, 15 suspects were arrested and eight places were searched in Tirana, Albania. […] Beginning in 2018, the perpetrators managed two fraudulent electronic platforms, 'BrokerZ' and 'Globalix', which lured victims in Germany into investing in non-existent financial products that promised large benefits. Among those arrested is one of the alleged leaders of the scam." READ MORE

Source: European Commission

Date: 25 Mar 2022

European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework

"The European Commission and the United States announce that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the Schrems II decision of July 2020. […] It will provide a durable basis for trans-Atlantic data flows, which are critical to protecting citizens' rights and enabling trans-Atlantic commerce in all sectors of the economy, including for small and medium enterprises." READ MORE

Source: Europol

Date: 29 Mar 2022

Latvia and Lithuania detain 108 over multi-million euro call centre scam

"With the support of Europol and Eurojust, the Latvian State Police (Valsts policija) and the Lithuanian Police (Lietuvos Policija) have detained over 100 people in Riga and Vilnius on suspicion of being involved in an international call centre scam. On 24 and 25 March hundreds of officers, including special intervention teams, raided a total of three call centres belonging to the same organised crime group. Its members are accused of defrauding victims across the world." READ MORE

Source: US Department of Justice

Date: 25 Mar 2022

Cybercriminal Connected to Multimillion Dollar Ransomware Attacks Sentenced for Online Fraud Schemes

"An Estonian man was sentenced today to 66 months in prison for his years-long role in furthering and facilitating computer intrusions, the movement of fraudulently obtained goods and funds, and the monetization of stolen financial account information. He also participated in ransomware attacks causing over $53 million in losses and was ordered to pay over $36 million in restitution. […] According to court documents, […] investigators uncovered within his electronic devices evidence of his involvement in ransomware activities. The post-extradition investigation determined that Berezan had participated in at least 13 ransomware attacks, seven of which were against U.S. victims, and that approximately $11 million in ransom payments flowed into cryptocurrency wallets that he controlled." READ MORE

Source: Computer Weekly

Date: 25 Mar 2022

European Commission proposes new cyber security regulations

"The European Commission (EC) has proposed two new regulations to establish common cyber and information security measures across the bloc, with the aim of bolstering resilience and response capacity against a range of cyber threats. Under the proposed cybersecurity regulation, which was published 22 March 2022, all European Union (EU) institutions, bodies, offices, and agencies will be required to have cyber security frameworks in place for governance, risk management, and control." READ MORE

Source: Next Inpact

Date: 29 Mar 2022

Au Conseil constitutionnel, le secret défense dans la captation des données informatiques

"Le Conseil constitutionnel dira le 8 avril prochain si les autorités françaises ont pu « pirater » les terminaux sécurisés EncroChat sans malmener les textes fondateurs. Une captation rendue possible par une disposition qui permet le recours à des moyens sous le secret de la défense nationale. […] S'en suivaient de nombreuses saisies de drogues, d'armes et autres avoirs outre des arrestations en France, mais aussi à l'étranger. Au-delà des faits, cette intervention a été rendue possible par l'article 706-102-1 du Code de procédure pénale, lequel autorise le procureur de la République ou le juge d'instruction à prescrire le recours aux moyens de l'État « soumis au secret de la défense nationale ». Ce texte dresse ainsi un pont entre le judiciaire et la trousse à outils des services du renseignement pour épauler les enquêtes ou instructions en cours." READ MORE

RELATED ARTICLE:

Kiratas, Federal Court of Justice: EncroChat data may be used, 25 March 2022

Source: US Department of Justice

Date: 24 Mar 2022

Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide

"The Department of Justice unsealed two indictments today charging four defendants, all Russian nationals who worked for the Russian government, with attempting, supporting and conducting computer intrusions that together, in two separate conspiracies, targeted the global energy sector between 2012 and 2018. In total, these hacking campaigns targeted thousands of computers, at hundreds of companies and organizations, in approximately 135 countries. […] "Russian state-sponsored hackers pose a serious and persistent threat to critical infrastructure both in the United States and around the world," said Deputy Attorney General Lisa O. Monaco." READ MORE

RELATED ARTICLE:

The Guardian, US charges four Russian hackers over cyber-attacks on global energy sector, 24 March 2022

Source: FBI

Date: 30 Mar 2022

Global Operation Disrupts Business Email Compromise Schemes

"The U.S. Department of Justice and international law enforcement partners carried out Operation Eagle Sweep over a three-month period and arrested 65 suspects in the United States and overseas, including 12 in Nigeria, eight in South Africa, two in Canada, and one in Cambodia. In parallel with Operation Eagle Sweep, Australia, Japan, and Nigeria conducted local operations targeting BEC actors. […] Starting in September 2021, Operation Eagle Sweep targeted BEC scammers believed responsible for targeting over 500 U.S. victims and for causing losses exceeding $51 million." READ MORE

Source: Krebsonsecurity

Date: 29 Mar 2022

Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"

"There is a terrifying and highly effective "method" that criminal hackers are now using to harvest sensitive customer data from Internet service providers, phone companies and social media firms.It involves compromising email accounts and websites tied to police departments and government agencies, and then sending unauthorized demands for subscriber data while claiming the information being requested can't wait for a court order because it relates to an urgent matter of life and death." READ MORE

Source: Ministerio Publico de Costa Rica

Date: 25 Mar 2022

MP participa en reunión de la Red Intenacional de Formadores Juciales

"La Unidad de Capacitación y Supervisión (UCS) del Ministerio Público (MP) formó parte de la reunión de avance y progreso de la Red Internacional de Formadores Judiciales, en la que se abordó el tema del ciberdelito y las pruebas electrónicas. En la actividad participaron 45 integrantes de dicha Red." READ MORE

RELATED ARTICLE:

Council of Europe, Plenary meeting: Judicial Trainers on Cybercrime and E-Evidence gather to discuss medium term priorities of International Network of National Judicial Trainers, 24 March 2022

Source: Globo São Paolo

Date: 30 Mar 2022

Tribunal Federal da 3ª Região, em São Paulo, é alvo de ataque hacker e tem trabalhos suspensos nesta quarta

"[…] Por causa do ataque hacker, os trabalhos no tribunal estão temporariamente suspensos, sem data ou hora para o retorno das atividades, segundo um comunicado divulgado pelo próprio tribunal. A Polícia Federal esteve no prédio do tribunal no final da tarde analisando a extensão do ataque hacker e vai abrir inquérito para investigar a ação ilegal. Apesar da página do TRF-3 na internet estar fora do ar, apenas com a exibição de um comunicado geral, a corte disse que o ataque não comprometeu os dados armazenados pelo órgão." READ MORE

Source: Diario Juridico

Date: 16 Mar 2022

Chile – Proyecto que moderniza normas sobre delitos informáticos

"El Senado respaldó el informe de la Comisión Mixta en torno al proyecto que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Ahora, el informe de la Mixta deberá ser ratificado por la Cámara de Diputadas y Diputados. Cabe recordar que el proyecto tiene por finalidad actualizar la legislación chilena en materia de delitos informáticos y ciberseguridad, adecuándola tanto a las exigencias del Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como «Convenio de Budapest», del cual Chile es parte." READ MORE

Source: Modern Ghana

Date: 23 Mar 2022

Africa needs effective policies to tackle cybercrime – Deputy Communications Minister

"Deputy Communications and Digitalisation Minister, Ama Pomaa Boateng has said, the growing problem of cybercrime in Africa requires countries to build effective laws, policies, and international cooperation frameworks together with the aim of solving the issue to the best satisfaction. […] Acting Director-General of the Cyber Security Authority (CSA), Dr. Albert Antwi Boasiako in his welcome address said fighting cybercrime would require a multi-stakeholder approach, with the collaboration of all relevant parties." READ MORE

Source: Investir au Cameroun

Date: 28 Mar 2022

Face aux ravages de la cybercriminalité, le Cameroun veut renforcer son dispositif de répression

"L'Assemblée nationale camerounaise est appelée à se prononcer sur un projet de loi autorisant le président de la République à ratifier la convention de Budapest sur la cybercriminalité, signée en novembre 2001. D'après l'exposé des motifs de ce projet de loi défendu le 25 mars 2022 par la ministre des Postes et Télécommunications, Minette Libom Li Likeng (photo), la ratification de cette convention permettra au Cameroun de s'arrimer aux standards internationaux en matière de lutte contre la cybercriminalité. " READ MORE

Source: Council of Europe

Date: 15 Mar 2022

CyberSouth: National workshop on the development of a domestic toolkit for first responders to cybercrime investigations in Morocco

"The series of workshops on the development of a domestic toolkit for first responders to cybercrime investigations, organised within the framework of the CyberSouth project, continued with the meeting organised on the 15th of March 2022 for the Moroccan authorities. […] Topics like the concept of first responders, the assistance for the victims or the protection of evidence integrity were covered during the workshop and a significant part of the presentation was dedicated to the Guide for first responders to cybercrime investigations." READ MORE

Source: Council of Europe

Date: 24 Mar 2022

GLACY+: Supporting the drafting of Philippines' new cybercrime strategy

"On 23-24 of March an online workshop was organised by the GLACY+ project for the key stakeholders from the Philippines in support of the finalisation of the country's draft National Cybercrime Strategy. The activity was initiated by the Philippines authorities and follows an advisory mission in 2019, where a draft strategy was analysed and recommendations for further improvement were provided, also with the assistance of the GLACY+ project." READ MORE

Source: Krebsonsecurity

Date: 17 Mar 2022

Pro-Ukraine 'Protestware' Pushes Antiwar Ads, Geo-Targeted Malware

"Researchers are tracking a number of open-source "protestware" projects on GitHub that have recently altered their code to display "Stand with Ukraine" messages for users, or basic facts about the carnage in Ukraine. The group also is tracking several code packages that were recently modified to erase files on computers that appear to be coming from Russian or Belarusian Internet addresses." READ MORE

Source: Forbes

Date: 28 Mar 2022

'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider

"A "powerful" cyberattack has hit Ukraine's biggest fixed line telecommunications company, Ukrtelecom. Described as the most severe cyberattack since the start of the Russian invasion in February, it has sent the company's services across the country down. […] The attack has only been acknowledged by Ukrtelecom in responses to customer comments on Facebook. […]NetBlocks, which tracks internet downtimes across the world, found Ukrtelecom had been dealing with a disrupted service since this morning, "collapsing to 13% of pre-war levels." READ MORE

Source: Krebsonsecurity

Date: 15 Mar 2022

Lawmakers Probe Early Release of Top RU Cybercrook

"Aleksei Burkov, a cybercriminal who long operated two of Russia's most exclusive underground hacking forums, was arrested in 2015 by Israeli authorities. The Russian government fought Burkov's extradition to the U.S. for four years — even arresting and jailing an Israeli woman to force a prisoner swap. That effort failed: Burkov was sent to America, pleaded guilty, and was sentenced to nine years in prison. But a little more than a year later, he was quietly released and deported back to Russia. Now some Republican lawmakers are asking why a Russian hacker once described as "an asset of supreme importance" was allowed to shorten his stay." READ MORE

Source: The Guardian

Date: 30 Mar 2022

11 years, 10 arrests, at least 62 women: how did Britain's worst cyberstalker evade justice for so long?

"Across England and Wales, police consistently fail to bring charges against stalkers. "Only 11% of reports of stalking result in a charge," says Alvarez. Even when the stalker is charged, conviction rates are abysmal. "Just 0.1% of cases result in a conviction," says Alvarez. This is despite the fact that many stalkers go on to commit further crimes. […] Cyberstalking is on the rise. Calls to the National Stalking Helpline about it have increased 20% since the start of the pandemic. Stalkers are taking advantage of our increasingly digitised lives to target victims through spyware, drones and even smart kettles and CCTV." READ MORE

Source: Council of Europe

Date: 17 Mar 2022

Cooperation on Cybercrime: exchange of views with the diplomatic community in Romania

"The Embassy of Italy and the Cybercrime Programme Office of the Council of Europe (C-PROC) held an exchange of views with the diplomatic community in Romania on current threats and challenges of cybercrime and new opportunities for cooperation. The event was held in Bucharest on 17 March within the framework of the Italian Presidency of the Council of Europe's Committee of Ministers." READ MORE

Source: Clubic France

Date: 22 Mar 2022

Cybercriminalité : avec la loi LOPMI, le gouvernement veut franchir un cap contre les ransomwares

"Le nouveau projet de loi de transformation numérique du ministère de l'Intérieur fait la part belle à la lutte contre la cybercriminalité, avec notamment, en ligne de mire, celle menée contre les rançongiciels et la naissance de l'application Ma Sécurité. " READ MORE

Source: City A.M.

Date: 24 Mar 2022

UK: Crypto fraud up 64 per cent as investment spikes for mainstream

"Crypto investment fraud in the UK has continued to rise sharply in the UK with a total of 9,458 cases reported in 2021, up 64 per cent, according to data from Pinsent Masons. Despite the volatility of cryptocurrencies and warnings by regulators of scams and other risks in the sector, crypto assets have been seen as an increasingly mainstream investment, again helping cryptocurrency related fraudsters." READ MORE

Latest reports

- FBI, Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability, 15 March 2022
- IMF Working Papers, Digitalization-and-Tax-Compliance-Spillovers-Evidence-from-a-VAT-e-Invoicing-Reform-in-Peru, 18 March 2022
- Police 1, To maximize resources, look to the cloud, 18 March 2022
- FBI - Internet Crime Complaint Center (IC3), 2021 Internet Crime Report, 22 March 2022
- ASPI, The UN norms of responsible state behaviour in cyberspace, 22 March 2022
- i-Sight Software, 15 Types of Evidence and How to Use Them in a Workplace Investigation, 24 March 2022
- Cyber Scoop, The long, bumpy road to cyber incident reporting legislation — and the one still ahead, 24 March 2022
- Cyberscoop, Bigger demands, bigger payouts are the trend in ransomware, 24 March 2022
- Bitdefender Threat Debrief, Highlight of the month: Ukraine Conflict, 24 March 2022
- SecureList, Phishing-kit market: what's inside "off-the-shelf" phishing packages, 24 March 2022
- Hackread, HubSpot Data Breach – Major Cryptocurrency Companies Impacted, 24 March 2022
- LexisNexis Risk Solutions, Cybercrime Report, July to December 2021, 28 March 2022
- CIO Tech Asia, Cybercrime report shows human initiated increased, 28 March 2022
- ENISA, European Cybersecurity Month 2021 - Deployment report, 28 March 2022
- EUROPEAN COURT OF AUDITORS, Special report 05/2022: Cybersecurity of EU institutions, bodies and agencies : Level of preparedness overall not commensurate with the threats, 29 March 2022
- Vie publique, Les cybermalveillances en forte hausse en 2021, 30 March 2022
- ASPI Special Report, UK, Australia and ASEAN cooperation for safer seas. A case for elevating the cyber–maritime security nexus, March 2022
- ASPI, Understanding global disinformation and information operations, March 2022

Upcoming events

- 4-7 April 2022, C-PROC/MONTENEGRO, (*in-person*), Regional training of trainers on delivery of the Specialised Judicial Training Course on Electronic Evidence, iPROCEEDS-2
- 5-7 April, C-PROC/ITALY (*online*), Participation in the Privacy Symposium, OCTOPUS
- 7 April, C-PROC/HELP, (*online*), Launch of the HELP course on cybercrime and electronic evidence, OCTOPUS
- 12-14 April 2022, C-PROC/ALBANIA and KOSOVO*, (*in-person*), Training Course on Financial Investigations, Virtual Currencies and Darknet, iPROCEEDS-2
- 14 April, C-PROC, *(online),* Series of monthly thematic webinars for the International Network of the National Judicial Trainers, GLACY+
- 15 April, C-PROC, (*desk review*), Revision and publication of a series of OCSEA country profiles onto the Octopus platform, OCTOPUS
- Starting in April, C-PROC, (*desk review*), Study on the First Additional Protocol highlighting the good practices in legislation, OCTOPUS
- April-May, C-PROC, (*desk review*), Translation into French, Spanish and Portuguese of the "Training skill certification Programme for judges and prosecutors delivering Council of Europe judicial trainings on cybercrime and electronic evidence", OCTOPUS
- April-June, C-PROC, (*desk review*), Further development of the online training platform on cybercrime and electronic evidence, OCTOPUS

The Cybercrime Digest appears bi-weekly. The news is selected by relevance to the current areas of interest to C-PROC and does 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