Cybercrime Digest

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

1 – 15 March 2022

Source: Council of Europe

Date: 15 Mar 2022

Council of Europe leaders make joint statement on the exclusion of the Russian Federation from the Council of Europe

The Italian Minister for Foreign Affairs and International Cooperation and Chair of the Council of Europe's Committee of Ministers, Luigi Di Maio, the President of the Council of Europe's Parliamentary Assembly, Tiny Kox, and the Secretary General of the Council of Europe, Marija Pejčinović Burić, have made the following statement: "As leaders of the Council of Europe we expressed on several occasions our firm condemnation of the Russian Federation's aggression against Ukraine. This unjustified and unprovoked aggression led to the decision of the Committee of Ministers and the Parliamentary Assembly to initiate the procedure of expulsion of the Russian Federation from the Council of Europe provided under Article 8 of the Statute. In this framework, tonight, the Parliamentary Assembly unanimously considered that the Russian Federation should no longer be a member State of the Organisation. The Committee of Ministers will hold an extraordinary meeting tomorrow morning also in the light of today's notification by the Minister of Foreign Affairs of the Russian Federation of the Russian leadership's decision to withdraw from the Council of Europe." READ MORE

RELATED ARTICLES:

Council of Europe, PACE to debate the consequences of the Russian Federation's aggression against Ukraine at an extraordinary session, 14-15 March 2022

Council of Europe, Secretary General condemns the Russian Federation's aggression, calls for solidarity with Ukraine, 14 March 2022

Source: The Guardian

Date: 4 Mar 2022

Russia blocks access to Facebook and Twitter

"Russia has completely blocked access to Facebook in retaliation for the platform placing restrictions on state-owned media. The Russian state communications regulator, Roskomnadzor, later said it had also restricted access to Twitter. Facebook and its sister platform Instagram have removed Russia Today (RT) and Sputnik from their output in the European Union this week and did the same with the UK on Friday, which drew an immediate response from the Russian communications regulator." READ MORE

RELATED ARTICLES:

Bloomberg, Russia Asks Court to Label Facebook, Instagram 'Extremist', 11 March 2022

Euronews, Meta says you can't call for Putin's death on Facebook over the war in Ukraine after all, 14 March 2022

Source: CNBC

Date: 14 March 2022

'For the first time in history anyone can join a war': Volunteers join Russia-Ukraine cyber fight

Cyber warfare related to the Ukraine-Russia conflict is surging as digital volunteers from around the world enter the fight. The number of cyberattacks being waged by — and on behalf of — both countries since the outbreak of the war is "staggering," according to the research arm of Check Point Software Technologies. "For the first time in history anyone can join a war," said Lotem Finkelstein, head of threat intelligence at Check Point Software. "We're seeing the entire cyber community involved, where many groups and individuals have taken a side, either Russia or Ukraine." […] In the first three days following the invasion, online attacks against Ukrainian military and governmental sectors increased by 196%, according to Check Point Research (CPR). They also modestly increased against Russian (4%) and Ukrainian (0.2%) organizations, according to the data, while simultaneously falling in most other parts of the world. READ MORE

RELATED ARTICLES:

BBC, Ukraine says it is fighting first 'hybrid war', 4 March 2022

Thailand Business, Thailand Warns of Increased Cyber Threats Amid Russia-Ukraine Conflict, 6 March 2022

Reuters, China says U.S. addresses used its computers to launch cyberattacks on Russia, Ukraine, 11 March 2022

The Guardian, We are not ready: a cyber expert on US vulnerability to a Russian attack, 11 March 2022

Source: CircleID

Date: 1 Mar 2022

Ukrainian Representatives to ICANN Ask for Russia's Domain to Be Revoked

"A letter sent to ICANN and IANA by a Ukrainian representative to ICANN's Government Advisory Council (GAC) asks for urgent and strict sanctions against the Russian Federation in "the field of DNS regulation." The letter urges ICANN to permanently or temporarily revoke Russia's top-level domains ".ru", ".рф" and ".su" and to shut down DNS root servers located in Saint Petersburg and Moscow. ICANN is also asked to assist in revoking SSL certificates for the Russian domains." READ MORE

Source: BBC

Date: 15 Mar 2022

Germany warns against Russian anti-virus use

"Germany's cyber-security authority has warned against using anti-virus software from Russian headquartered company Kaspersky. The Federal Office for Information Security (BSI) issued the statement in light of the conflict in Ukraine. Russian information-technology businesses could be spied on or forced to launch cyber-attacks, it said. Kaspersky told BBC News the warning had been "made on political grounds" and it had no ties to the Russian government. The BSI made no allegation of current problems with Kaspersky's products but said the conflict in Ukraine and Russian threats against the European Union, Nato and Germany brought with them the risk of cyber-attacks." READ MORE

Source: Roll Call

Date: 8 Mar 2022

United States: Lawmakers fear cryptocurrencies could be back door for sanctioned rubles

"Lawmakers on both sides of the aisle are worried about the potential of cryptocurrency to serve as an escape hatch for sanctioned Russian money, with some saying the risk hastens the need for legislation. The anonymity provided by bitcoin and other cryptocurrencies could undermine the effectiveness of sanctions against Russia after its invasion of Ukraine, the lawmakers say. Industry advocates, however, say the technology provides greater transparency for law enforcement and warn against an overreaction by Congress and regulators." READ MORE

Source: eff.org

Date: 3 Mar 2022

Negotiations Over UN Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights

"While tensions run high across the globe over the invasion of Ukraine, the world's governments are meeting at the UN this week and next to find common ground on a proposed treaty to facilitate international cooperation and coordination in computer crime investigations. The treaty, if approved, may reshape criminal laws and bolster cross-border police surveillance powers to access and share user data, implicating the privacy and human rights of billions of people worldwide." READ MORE

RELATED ARTICLES:

ICCLR, Canada's Position at the UN Cybercrime Treaty Negotiations, 2 March 2022

The interpreter, The hypocrisy of Russia's push for a new global cybercrime treaty, 7 March 2022

La silla vacia, En la ONU se está decidiendo la política criminal de internet, 8 March 2022

Source: Interpol

Date: 14 Mar 2022

Experts highlight global efforts to combat online child sexual abuse

"With the scale of child sexual exploitation and abuse increasing, specialists from around the globe have gathered to enhance the collective global response. Over four days (14 - 17 March), the INTERPOL Specialists Group on Crimes Against Children will engage participants in global efforts and technical solutions to combat online child sexual abuse, identify victims and their attackers, and disrupt criminal networks involved in producing and circulating abusive content. Some 98 participants from 54 countries, regional and international organizations, the private sector, NGOs and academia will come together for the first time since the COVID pandemic to share best practices across countries and sectors." READ MORE

Source: ebu.ch

Date: 4 Mar 2022

E-evidence: The EBU reiterates its support for the European Parliament approach ahead of next Council's meeting

"This Friday, EU ministers of the Justice and Home Affairs Council will discuss the draft regulation on European production and preservation orders for electronic evidence in criminal matters (eEvidence proposal). The proposed new rules aim to adapt evidence gathering for the internet age in the context of cybercrime and to speed up cross border enforcement in criminal cases. While the EBU recognizes the importance of the initiative, we fear the Commission proposal risks a chilling effect on the media and on cross-border investigative journalism." The informal interinstitutional negotiations started more than a year ago now seem to have reached a serious dead end. To remedy this situation, the European Parliament Rapporteur presented a compromise package to the Council last December." READ MORE

Source: Europol

Date: 2 Mar 2022

146 children worldwide saved in an operation targeting child abuse online

"Europol supported an international investigation into tens of thousands of accounts possessing and sharing child sexual abuse material online. The operation, led by the Te Tari Taiwhenua Department of Internal Affairs, has so far involved law enforcement authorities from Australia, Austria, Canada, Croatia, Czechia, Greece, Hungary, Slovenia, Spain, the UK and the US. The international coordination of the investigative activities facilitated the identification of a large number of individuals tied to these accounts." READ MORE

Source: eff.org

Date: 3 Mar 2022

Cybersecurity Experts Urge EU Lawmakers to Fix Website Authentication Proposal That Puts Internet Users' Security and Privacy at Risk

"Electronic Frontier Foundation (EFF) technologists, along with 36 of the world's top cybersecurity experts, today urged European lawmakers to reject proposed changes to European Union (EU) regulations for securing electronic payments and other online transactions that will dramatically weaken web security and expose internet users to increased risk of attacks by cybercriminals. The ill-conceived proposed amendment to Article 45 in the EU's Digital Identity Framework (eIDAS) requires popular browsers like Firefox, Google, and Safari to accept flawed website certificates that bypass the rigorous security standards built into today's browsers to ensure user data isn't intercepted and stolen by criminals." READ MORE

Source: Le Monde

Date: 7 Mar 2022

Samsung Electronics victime d’une cyberattaque, les données de ses clients ne seraient pas concernées

“Samsung Electronics a été victime d’une cyberattaque et d’une fuite de données, a fait savoir par voie de presse le constructeur coréen lundi 7 mars. « Selon nos premières analyses, la fuite concerne une partie du code source relatif à nos [smartphones] Galaxy, mais n’inclut pas les informations personnelles de nos clients ni de nos employés », a expliqué un porte-parole du géant de l’électronique à Bloomberg. Dans son communiqué, l’entreprise affirme avoir pris les mesures pour prévenir ce genre d’incident à l’avenir. On ignore si les données volées ont fait l’objet d’une demande de rançon.” READ MORE

RELATED ARTICLE:

ZDNet, Samsung confirms Galaxy source code breach but says no customer information was stolen, 7 March 2022

Source: Council of Europe

Date: 7-9 Mar 2022

Octopus Project: Council of Europe organises a regional workshop on COVID-19-related cybercrime and electronic evidence in Asia

“The COVID-19 pandemic has been accompanied by a major surge in cybercrime and challenges related to electronic evidence. This is also true for Asia. The Council of Europe under its Octopus Project and in co-operation with the Information and Communication Technology Agency of Sri Lanka (ICTA) together with Sri Lanka CERT, therefore, held a regional workshop on this topic in Colombo, Sri Lanka, from 7 to 9 March 2022. This event was organised with the financial support of the Government of Japan. The workshop brought together some forty experts participating in person and representing criminal justice authorities of Laos, Malaysia, Maldives, Nepal, Philippines, Sri Lanka, the US Department of Justice and INTERPOL. In addition, experts from Japan, Indonesia and UNODC contributed online. The event resulted in a number of proposals to ensure a more effective criminal justice response to current COVID-19-related cybercrime and other crises and challenges that may occur in the future.” READ MORE

Source: The Diplomat

Date: 4 Mar 2022

Amendment to Pakistan’s Cybercrime Law Sparks Outrage From Free Speech Defenders

“Pakistani Prime Minister Imran Khan has defended recent amendments to the country’s controversial cybercrime laws, saying they were necessary to root out “fake news.” [...] Khan said the amendment to the Prevention of Electronic Crimes Act 2016, first introduced by Pakistan Muslim League-Nawaz (PML-N), was made to tackle filth such as child pornography and online harassment of women. Under the new law, which has been termed “draconian” and “undemocratic” by media bodies and human rights organizations, a person accused of defaming another person or institution, such as the army or judiciary, has now been denied the right to bail and could be jailed for up to five years instead of three.” READ MORE

Source: Colombo Gazette

Date: 9 Mar 2022

Sri Lanka: Personal Data Protection Bill passed with amendments

"The Personal Data Protection Bill was passed in Parliament today, with amendments. [...] The Bill aims to regulate the processing of personal data by identifying and strengthening the rights of data subjects – persons whose data is held by a processor or controller. However, Transparency International Sri Lanka (TISL) had said earlier that it remains deeply concerned about three key areas in the Bill including the impact on certain rights and freedoms, if enacted in its current form. The creation of a legal framework on personal data protection can be viewed as an important step in safeguarding human rights, especially at a time when information has become both a tool to be used by the people and against them." READ MORE

RELATED ARTICLE:

Economynext, Sri Lanka parliament passes data protection act amid privacy concerns, 10 March 2022

Source: Council of Europe

Date: 15 March 2022

GLACY+: Workshop for Ugandan Authorities on the harmonisation of cybercrime legislation and electronic evidence with international standards

"On 15 March 2022, the Council of Europe, through the GLACY + project, held an interactive workshop with Ugandan authorities on harmonising national legislation on cybercrime and electronic evidence with international standards[...]. The workshop was organised in collaboration with the Ugandan Ministry of Information and Communication Technology and the Office of the Director of Public Prosecutions, and brought together members of the national Task Force mandated to update the existing legislation on cybercrime and harmonise it with existing international standards, and other stakeholders [...]. During the workshop, participants discussed the findings and recommendations of the analysis of national cybercrime legislation conducted by the Council of Europe expert, and identified the key areas of legislative reforms to be addressed by the National Taskforce. The workshop followed the previous advisory mission on legislation organised in Uganda under the GLACY+ project in 2018." READ MORE

Source: Council of Europe

Date: 3 Mar 2022

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

"The series of workshops on the development of a domestic toolkit for first responders to cybercrime investigations recently launched within the CyberSouth project continued, on the 2nd of March 2022, with an online meeting for the Algerian authorities. In the given international context, strengthening of criminal justice capacities to fight cybercrime is more relevant than ever. Algerian representatives of police and gendarmerie actively participated in the discussions, presenting the structure of their units and procedural aspects on reporting cybercrime offences and initiation of criminal investigations. Recommendations on the harmonisation with international standards followed. An important topic of discussion was the relevance of a domestic toolkit for first responders to cybercrime investigations, concept and responsibilities." READ MORE

Source: Infogate

Date: 14 Mar 2022

Chile: Avanza modernización de Ley de Delitos Informáticos ajustándose al Convenio de Budapest

"El Senado -al que le queda poca vida- aprobó el informe de la Comisión Mixta que zanjó las diferencias suscitadas entre ambas Cámaras (Senado y Diputados) 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. Cabe recordar que el proyecto tiene por objeto 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, y en cuanto a la evolución de las tecnologías de la información y la comunicación, todo ello para dar un tratamiento más comprensivo del contexto en que se cometen estos ilícitos y subsanar la carencia de medios suficientes para su investigación." READ MORE

Source: Insight Crime

Date: 9 Mar 2022

Dominican Republic Cybercrime Ring Shows Extent of Caribbean's Financial Fraud Crisis

"The Dominican Republic has dismantled a transnational cybercrime network believed to have defrauded hundreds of US citizens to the tune of more than $200 million, in just the latest example of the growing threat posed by financial crime operations in the Caribbean. Hundreds of law enforcement officials carried out a series of raids March 2 as part of Operation Discovery, an investigation authorities started more than a year ago to break up a criminal network that allegedly defrauded its victims via economic and sexual extortion, as well as identity theft, according to an official press release." READ MORE

Source: Europol

Date: 10 Mar 2022

New Accountability Framework to use artificial intelligence in a transparent and accountable manner

"The project Accountability Principles for Artificial Intelligence (AP4AI) is jointly conducted by Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) and the Europol Innovation Lab, and supported by Eurojust, the EU Agency for Asylum (EUAA) and the EU Agency for Law Enforcement Training (CEPOL) with advice and contributions by the EU Agency for Fundamental Rights (FRA), in the framework of the EU Innovation Hub for Internal Security. The ambition of the AP4AI project is to create a practical toolkit that directly and meaningfully supports AI Accountability when implemented in the internal security domain." READ MORE

Source: Council of Europe

Date: 7-11 Mar 2022

CyberEast and iProceeds-2 projects of the Council of Europe in partnership with Cybersecurity East project organised a Cyber Exercise for East and South-East European countries

"CyberEast and iProceeds-2 projects, funded by the European Union and the Council of Europe, in partnership with the Cybersecurity EAST project funded by the European Union, organised during 7-11 March 2022 in Athens, Greece a Regional Cyber Exercise focused thematically on cooperation between the cybersecurity community (primarily CSIRTs) with the law enforcement in handling and investigating a malware attack orchestrated by a criminal group. The exercise brought together 40 experts from East and South-East European countries under the guidance of a team of international experts and the exercise partners of TR-CERT(USOM), Turkey." READ MORE

RELATED ARTICLE:

Le monde Informatique, L'UE lance un exercice de cybersécurité pour les pays d'Europe orientale et du Sud-Est, 3 March 2022

Source: Euractiv

Date: 11 Mar 2022

Conference on the Future of Europe: citizens ask adapting legislation to digitalisation, future pandemics, and wars

"Preparing schools for pandemics and wars, fighting cybercrime and disinformation, and getting society accustomed to digitalisation are some of the approved suggestions from the conference on the future of Europe (CoFoE) meeting at the end of February in Dublin. A total of 48 recommendations were proposed and approved by participants in the EU's first deliberative democracy experiment, which aims to involve European citizens in EU policy-making." READ MORE

Latest reports

- Brussels Times, Belgium 4th in world for cybercrime, 1 March 2022
- APEX Privacy, Why Investors Should Care About Cyber Security, 2 March 2022
- Reuters, Prosecutors and digital evidence: Cloud-based technologies offer a solution, 2 March 2022
- Google Threat Analysis Group, An update on the threat landscape, 7 March 2022
- ENISA Europa, Report on CSIRT-Law Enforcement Cooperation, 8 March 2022
- Africa Center for Strategic Studies, African Lessons in Cyber Strategy, 8 March 2022
- Simplilearn, Top 10 Cybersecurity Trends to Watch Out For in 2022, 8 March 2022
- Pressperu.com, ¿Cuál Es La Situación Actual De La Mujer En La Industria De La Ciberseguridad?, 8 March 2022
- Infinty.eu, Key Steps to Managing a Cybercrime Scene, 9 March 2022
- Cisco Talos, Threat advisory: Cybercriminals compromise users with malware disguised as pro-Ukraine cyber tools, 9 March 2022
- Agence nationale de la sécurité des systèmes d'information, Panorama de la menace informatique 2021, 9 March 2022
- Proofpoint, Mobile Malware is Surging in Europe: A Look at the Biggest Threats, 9 March 2022
- APEX Privacy, 7 Ways To Boost Your Cyber Resilience, 9 March 2022
- ENISA Europa, Cyber Threats Outreach In Telecom, 10 March 2022
- Stuff New Zealand, $6.6 million lost to cyber crime in the December quarter, 10 March 2022
- Krebsonsecurity.com, Recent 10x Increase in Cyberattacks on Ukraine, 11 March 2022
- Security Brief, Five data fundamentals to quash cybercrime, 14 March 2022
- Accenture Cyber Threat Intelligence (ACTI), Global Incident Report: Threat Actors Divide Along Ideological Lines over the Russia-Ukraine Conflict on Underground Forums, 14 March

Upcoming events

- 16 March, C-PROC/TUNISIA, (*online*), National Workshop on the development of a domestic toolkit for first responders to cybercrime investigations, CyberSouth
- 17 March, C-PROC, (*in-person*), Promotion of the Second Additional Protocol and cybercrime capacity building prorammes among the diplomatic community, OCTOPUS
- 22-25 March, C-PROC/LEBANON, (*in-person*), Judicial ToT on cybercrime and e-evidence for magistrates, CyberSouth
- 23 March, C-PROC/NAURU, (*online*), Support for the legislative reform on cybercrime - workshop on procedural powers, GLACY+
- 23-24 March, C-PROC/PHILIPPINES, (*hybrid*), Advisory mission on national cybercrime strategy, GLACY+
- 24-March, C-PROC, (*online*), Plenary of the international Network of Judicial Trainers, GLACY+
- 23-25 March, C-PROC/ALBANIA, (*online*), Practical exercise bringing together cybercrime, cybersecurity and the private sector aimed at developing practical skills of public-private cooperation, iPROCEEDS-2
- 28-31 March, C-PROC/ALGERIA, (*in-person*), Judicial ToT on cybercrime and e-evidence for magistrates, CyberSouth
- 30 March, C-PROC/BOSNIA AND HERZEGOVINA, (*in-person*), Service Providers and LEA Cooperation on conducting cyber-criminal investigations Conference, iPROCEEDS-2
- 30 March-01 April, C-PROC/MONTENEGRO, (*in-person*), Training skill certification programme for judges and prosecutors delivering Council of Europe judicial training on cybercrime and electronic evidence, iPROCEEDS-2

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