Cybercrime Digest

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

1 – 15 May 2022

Source: Council of Europe

Date: 12 May 2022

Enhanced co-operation and disclosure of electronic evidence: 22 countries sign new Protocol to Cybercrime Convention

"The Second Additional Protocol to the Convention on Cybercrime (Budapest Convention), aimed at enhancing co-operation and disclosure of electronic evidence has been opened for signature at a conference organised under the Italian Presidency of the Council of Europe's Committee of Ministers.

The Protocol was signed in the presence of several ministers by the following Council of Europe member states: Austria, Belgium, Bulgaria, Estonia, Finland, Iceland, Italy, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Portugal, Romania, Serbia, Spain and Sweden, and by non-member states: Chile, Colombia, Japan, Morocco and United States." READ MORE

RELATED ARTICLES:

DataGuidance, International: 22 states sign new additional protocol to Cybercrime Convention, 13 May 2022

El Universo, Varios Estados firman el protocolo del Convenio contra cibercrimen, 12 May 2022

Council of Europe, Speech of the Secretary General - Conference and Opening for Signature of the 2nd Additional Protocol to the Convention on Cybercrime, 12 May 2022

Council of Europe, Enhanced co-operation and disclosure of electronic evidence: 22 countries open the way by signing the Second Additional Protocol to the Cybercrime Convention, 12-13 May 2022

Cancilleria de Colombia, Colombia a la vanguardia de los procesos internacionales que buscan robustecer mecanismos para prevenir y perseguir el delito cibernético, 17 May 2022

Source: CORCOM

Date: 12 May 2022

Italy: Cartabia firma il trattato per un accesso più veloce alle prove

"La ministra della Giustizia Marta Cartabia ha firmato a Strasburgo, alla riunione del Consiglio d'Europa, il protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica. Due gli obiettivi fondamentali del trattato, ha spiegato Cartabia: "Rafforzare la cooperazione nel campo della lotta alla criminalità informatica e consolidare la raccolta di prove di reati in forma elettronica ai fini di specifiche indagini o procedimenti penali." READ MORE

Source: United States Department of Justice

Date: 12 May 2022

United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime

"At the Council of Europe (COE) headquarters in Strasbourg, France, on May 12, Deputy Assistant Attorney General (DAAG) Richard Downing of the U.S. Department of Justice's Criminal Division signed the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence on behalf of the U.S. government. This strengthening and expansion of the multilateral international treaty commonly called the Budapest Convention is part of the United States' steadfast commitment to helping nations, including the United States, fight cybercrime by obtaining access to needed electronic evidence." READ MORE

Source: Ministerio de Relaciones Exteriores

Date: 12 May 2022

Chile firma el Segundo Protocolo Adicional al Convenio de Budapest

"Con fecha 12 de mayo, Chile suscribió el Segundo Protocolo Adicional al Convenio de Budapest sobre Ciberdelincuencia. El acto se realizó durante la ceremonia de apertura para la firma del texto en la sede del Consejo de Europa en Estrasburgo. Durante la ceremonia, veintidós países miembros del Convenio de Budapest suscribieron el documento. La delegación de Chile estuvo conformada por representantes de la División de Seguridad Internacional y Humana de Minrel, y de la Fiscalía Nacional." READ MORE

Source: Government of Portugal

Date: 12 May 2022

Ministra da Justiça assina segundo Protocolo à Convenção sobre Cibercrime em nome da República Portuguesa

"Catarina Sarmento e Castro participou na cerimónia de abertura da assinatura do Segundo Protocolo Adicional à Convenção sobre Cibercrime, também conhecida como Convenção de Budapeste, que decorre até amanhã em Estrasburgo. No seu discurso, a Ministra da Justiça reafirmou o empenho de Portugal na prevenção e na luta contra a criminalidade, particularmente a cibercriminalidade, tendo em conta os seus efeitos negativos na segurança e bem-estar dos cidadãos, no pleno gozo dos direitos humanos nas sociedades democráticas e no Estado de direito, bem como a importância que constitui a Convenção sobre Cibercrime para uma cooperação internacional ativa e eficaz na investigação da cibercriminalidade." READ MORE

Source: Kingdom of Morocco

Date: 13 May 2022

Morocco Signs Second Additional Protocol to Budapest Cybercrime Convention

"Morocco signed, on Thursday in Strasbourg, the 2nd Additional Protocol to the Budapest Convention on Cybercrime on enhancing cooperation and disclosure of electronic evidence. […] This protocol, which aims to complement the said Convention, was signed at the Council of Europe by Minister of Justice Abdellatif Ouahbi, who leads a large delegation of his department, on the occasion of this conference, organized in cooperation with the Italian Presidency of the Committee of Ministers of the Council of Europe." READ MORE

Source : Ministerio de Justicia

Date : 12 May 2022

España firma el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia

"El embajador representante permanente de España en el Consejo de Europa, Manuel Montobbio, ha firmado hoy, en nombre del Estado español, el Protocolo adicional segundo al Convenio del Consejo de Europa sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas. El texto incluye herramientas dirigidas a facilitar la investigación de procesos penales que requieran de prueba electrónica transnacional." READ MORE

RELATED ARTICLE:

La Moncloa, Spain signs the Second Additional Protocol to the Convention on Cybercrime, 12 May 2022

Source: ICANN

Date: 5 May 2022

ICANN Develops Tool to Monitor and Combat Malicious Online Activities

"Domain Name System coordinator responds to the Internet Security Threats COVID and the Russia-Ukraine war pose for all users. In the midst of global crises, such as a pandemic or a war, malicious online activities typically increase. Bad actors seek new ways to install malware on devices without the user's consent to gather sensitive information or gain access to private computer systems. They also trick users into revealing sensitive personal, corporate or financial information – this is known as phishing. […] The Internet Corporation for Assigned Names and Numbers organization (ICANN) developed an evidence-based approach that identifies domain names that appear to have been used for malicious purposes and are related to the COVID-19 pandemic and the Russia-Ukraine war". READ MORE

Source: SChronicles

Date: 10 May 2022

Cybercrime Costs Global Economy More Than 6 Billion In 2021

"Cybercrime has cost the global economy more than $6 trillion, Alessandro Profumo, CEO of the Italian aerospace and defense giant, said on Tuesday. "The new threats that have been registered in the field of cybersecurity in the last two years are the 'collateral damage' caused by the Covid-19 epidemic and the acceleration of digitization," explained Profumo at the opening of an expert congress on cybertech in Rome Europe 2022 and the war in Ukraine. Cybersecurity has become a key issue for the European Commission and European Union (EU) members to ensure "digital sovereignty and strategic autonomy," she added." READ MORE

Source: VOA

Date: 4 May 2022

A Trove of Digital Evidence Documents War Crimes in Ukraine

"With the help of international experts, Ukraine rushes to collect evidence of widespread war crimes, using 21st century technology to bring perpetrators to justice. VOA's Veronica Balderas Iglesias reports. Warning: contains graphic images." READ MORE

Source: ZDNet

Date: 10 May 2022

Ransomware has gone down because sanctions against Russia are making life harder for attackers

"The number of ransomware attacks has gone down in recent months because sanctions against Russia are making it harder for cyber criminals to organise attacks and receive ransom payments, Rob Joyce, director of cybersecurity at the National Security Agency (NSA), has revealed. Ransomware attacks have long been a major cybersecurity issue for organisations around the world, affecting computer networks running critical infrastructure, hospitals, businesses and more. […]"One interesting trend we see is, in the last month or two, ransomware is actually down. There's probably a lot of different reasons why that is, but I think one impact is the fallout of Russia-Ukraine," said Joyce. "As we do sanctions and it's harder to move money and it's harder to buy infrastructure on the web, we're seeing them be less effective – and ransomware is a big part of that," he added." READ MORE

Source: BBC

Date: 12 May 2022

Ukraine war: Don't underestimate Russia cyber-threat, warns US

"There has been a sustained cyber-conflict over Ukraine which could still escalate, a senior US intelligence official has told the BBC. Despite warnings, major cyber-attacks on the West have so far not materialised. But Russia shouldn't be underestimated, Rob Joyce, director of cyber-security at the National Security Agency said. Meanwhile independent hackers targeting Russia in support of Ukraine could also spark escalation, he warned. "I'm still very worried about the threats emanating from around the Russia-Ukraine situation," Mr Joyce, one of America's most experienced cyber officials, said. Initial surprise that Russia did not launch an all-out cyber-assault to cripple Ukrainian infrastructure as the war began has been replaced by an understanding that there has been far more aggressive activity than first thought." READ MORE

RELATED ARTICLE:

Reuters, The cyber war between Ukraine and Russia: An overview, 10 May 2022

The Guardian, Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief, 10 May 2022

DW, Pro-Russia 'Killnet' hackers target Italian institutions, 11 May 2022

BBC, UK blames Russia for satellite internet hack at start of war, 11 May 2022

YLW, Finland should brace for Russian cyber-attacks, Traficom says, 12 May 2022

Source: Council of Europe

Date: 4 May 2022

C-PROC: International law enforcement training course on investigating ransomware attacks organised by the Council of Europe brings together 34 countries from different world's regions

"On 3 and 4 May 2022, the Council of Europe Cybercrime Programme Office (C-PROC) organised an online international law enforcement training course on investigating ransomware attacks. The event, which gathered around 120 practitioners from 34 countries (Algeria, Azerbaijan, Bangladesh, Bhutan, Burkina Faso, Burundi, Cameroon, Cote d'Ivoire, Ethiopia, Fiji, Gambia, Georgia, Ghana, Guinea, Indonesia, Jordan, Kenya, Kiribati, Lebanon, Malawi, Maldives, Mauritius, Moldova, Mauritius, Morocco, Nepal, Nigeria, Philippines, Rwanda, Thailand, Tunisia, Ukraine, Uganda, Vanuatu) aimed at strengthening the knowledge of participants on how to conduct criminal investigations and co-operate at international level on ransomware attacks." READ MORE

Source: Forbes

Date: 5 May 2022

United States: Biden Signs Bill To Create Cybercrime Reporting System

"President Joe Biden signed today the Better Cybercrime Metrics Act into law. The measure, which received bipartisan Congressional support, represents the latest step by the federal government to help beef up various aspects of the country's cyber defenses. The new law establishes requirements to improve the collection of data related to cybercrime and cyber-enabled crime. The new law comes in the midst of rising concerns and warnings about increased cyberattacks by Russia in response to the U.S.' support of Ukraine." READ MORE

RELATED ARTICLE:

Security Magazine, Better Cybercrime Metrics Act signed into law, 10 May 2022

Source : Insight Crime

Date : 3 May 2022

Major Ransomware Attacks in Peru and Costa Rica Spell More Trouble for Region

"A cybercrime group that has threatened to release troves of stolen data from the Costa Rican government has now hit Peru's intelligence agency, showing how governments in the region continue to be easy pickings for ransomware attacks. The Russian cybercrime group known as Conti announced on April 27 that it had hacked the website of Peru's National Directorate of Intelligence, local media outlet La República reported. The group has threatened to publish stolen data, which it claims is sensitive, if the government did not pay a ransom. The group also warned that the private sector would also be targeted if it did not receive $10 million, reported El Observador. Costa Rica has thus far refused to pay." READ MORE

RELATED ARTICLE:

wtop.com, Costa Rica declares emergency in ongoing cyber attack, 12 May 2022

Source: Daily Express

Date: 1 May 2022

Trinidad and Tobago: Held to ransom by cyber attacks

"The sectors most hit by cyber-attacks in Trinidad and Tobago are Government, finance and manufacturing. In an interview with the Sunday Express last Friday, manager of the T&T Cyber Security Incident Response Team (TT-CSIRT) of the Ministry of National Security, Angus Smith, said over 2,600 Government e-mail accounts have been found in third party data breaches from 2008 to 2021. Noting the cybercrime legislation needs to be in line with the Budapest Convention, Smith said there are other conventions in which this country can become signatories, which will result in the synchronisation of legislation across countries in the world which have similar legislation." READ MORE

Source: La Tribuna de Albacete

Date: 4 May 2022

Colombia: La delincuencia informática es un fenómeno creciente

"En el año 2001, en el seno del Consejo de Europa, se puso en marcha el Convenio de Budapest contra el cibercrimen, al que se adhirió España en el año 2010. Se trata de un tratado internacional para luchar contra la delincuencia informática en todos sus aspectos, con el que se busca que todos los países que lo ratifican adecuen su legislación nacional a las normas del convenio. Cabe destacar que actualmente han suscrito el convenio Estados Unidos, Japón, todos los países europeos salvo Rusia y muchos países hispanoamericanos." READ MORE

Source : Krebsonsecurity

Date : 12 May 2022

United States: DEA Investigating Breach of Law Enforcement Data Portal

"The U.S. Drug Enforcement Administration (DEA) says it is investigating reports that hackers gained unauthorized access to an agency portal that taps into 16 different federal law enforcement databases. KrebsOnSecurity has learned the alleged compromise is tied to a cybercrime and online harassment community that routinely impersonates police and government officials to harvest personal information on their targets. On May 8, KrebsOnSecurity received a tip that hackers obtained a username and password for an authorized user of esp.usdoj.gov, which is the Law Enforcement Inquiry and Alerts (LEIA) system managed by the DEA." READ MORE

Source: Tribute South Africa

Date: 12 May 2022

Experts urge Africa to find a way forward on cybercrime

"Cyber experts are urging Africa to up its game in the face of criminals targeting the continent's fast-growing internet economy with scams and theft. Countries south of the Sahara are some of the world's fastest-growing online markets — which makes them both attractive and vulnerable to cybercrime, say specialists. "The issue of cybersecurity has to be raised to the core duties of the state," Chadian economist Succes Masra said at a cyber conference in Abidjan, Ivory Coast's economic hub, which ended on Tuesday. Half a billion people in Africa are connected to the internet, according to Interpol — a figure that in raw numbers places the continent ahead of other regions such as South America or the Middle East." READ MORE

Source: DW

Date: 13 May 2022

How cybercrime laws are used to silence dissent in Middle East

"The battlefield is gruesome, global and growing — cyberattacks have become a dangerous threat to governments, people and institutions all over the world. In response, around 80% of the world's countries have implemented cybercrime legislation, according to the United Nations Conference on Trade and Development. But in some Arab countries, these laws are increasingly misused by governments to silence dissent and curb freedom of speech. The latest example is Syria, where President Bashar Assad's government updated its cybercrime laws in April. The newly amended law 20/2022 targets both online and offline criticism of the president, state and constitution." READ MORE

Source : Intelligence Online

Date : 12 May 2022

West increases aid to boost Chisinau's cyber defence capacities

"Since the unrest in Transnistria at the end of April, the media and international community have kept an eye on Moldova. Intelligence agencies in the country are worried about their cyber capacities, despite a boost from Chisinau's Israeli and Western allies, which has increased in recent weeks." READ MORE

Source: Financial Conduct Authority

Date: 5 May 2022

United Kingdom: 'Sharing my screen cost me £48,000' – half of investors would miss signs of screen sharing scam as FCA warns of 86% increase

"New research from the FCA has found that nearly half (47%) of investors would fail to identify a screen sharing scam, as it reveals an increase of 86% in cases in one year, with 2,014 cases and over £25 million in loses. In one case, a 59-year-old who was persuaded to download remote desktop software to secure an investment, lost over £48,000 while scammers accessed her banking details, her pension, and applied for loans on her behalf. […] Using platforms including Teams, TeamViewer and Zoom, screen sharing scams not only involve consumers sharing their financial data – but scammers have also been able to embed themselves in victims' digital devices to access online banking and investment details." READ MORE

Latest reports

- Quantum Marketer, Cybercrime in Statistics: The History, the Records, and Safety Tips You Need to Know, 2 May 2022
- Google Threat Analysis Group, Update on cyber activity in Eastern Europe, 3 May
- National Cyber Security Centre, Threat report on application stores, 4 May 2022
- GovTech: Virginia Researchers Study Gaps in Cyber Crime Reporting, 4 May 2022
- FBI, Business Email Compromise: The $43 Billion Scam, 4 May 2022
- Top10VPN, Cybercrime Statistics 2022, 5 May 2022
- Eurojust, Eurojust Casework on Corruption: 2016-2021 Insights, 5 May 2022
- Atlas VPN, 60 Worrying Cybercrime Statistics & Facts, 8 May 2022
- VIDIZIMO, Role Of Digital Evidence Management System In Solving Crime, 10 May 2022
- EMBROKER, Common Types of Cybercrimes and How to Protect Your Business From Them, 10 May 2022
- The Guardian, UK cybersecurity unit tackles record number of online scams in 2021, 10 May 2022
- Joint Cybersecurity Advisory, Protecting Against Cyber Threats to Managed Service Providers and their Customers, 11 May 2022
- Europol, Crypto investment scams – infographic, 12 May 2022
- Just Security, On New Cross-Border Cybercrime Policing Protocol, a Call for Caution, 13 May 2022

Upcoming events

- 9 May-17 June, C-PROC/INTERPOL *(online),* FOSI Training course, GLACY+
- 16-19 May, C-PROC/ASEAN, *(hybrid),* Cybercrime Conference and Operational meeting, GLACY+
- 17 May, C-PROC, *(online),* E-Evidence Program for Prosecution (e-EPP): Module 2 - Legal framework of e-Evidence admissibility, GLACY+
- 17 May, C-PROC/ARMENIA, *(in person),* Forum of criminal justice, civil society and private sector on transparency of cybercrime action, CyberEast
- 18 May, C-PROC/LAC region, *(online),* Side event CCPCJ on importance of capacity building in Latin America and the Caribbean (LAC) Region, GLACY+
- 18 May, C-PROC/VANUATU, *(online),* Advisory mission on data protection legislation - debriefing session: legislative drafting WKS1, GLACY+
- 19-20 May, C-PROC/GEORGIA, *(in person),* Tabletop exercise for policy makers on critical infrastructure protection and cybercrime, CyberEast
- 23 May C-PROC, *(online),* Series of webinars on the 2nd Additional Protocol: Data Protection safeguards and principles in "cross-border" investigations, GLACY+
- 23-26 May C-PROC/MOROCCO, *(in person),* Training of trainers workshop on cybercrime and e-evidence for magistrates, CyberSouth
- 24 May, C-PROC/AZERBAIJAN, *(in person),* Forum of criminal justice, civil society and private sector on transparency of cybercrime action, CyberEast

- 24-26 May, C-PROC/NIGERIA, *(in person),* Advisory mission on search, seizure, and confiscation of online proceeds of crime, GLACY+
- 24-27 May, C-PROC/SIERRA LEONE, *(hybrid),* Support for the national delivery on the Introductory course on cybercrime and electronic evidence (jointly organized with OCWAR-C), GLACY+
- 25 May, C-PROC, *(in person),* Participation in the 15th International Conference on Computers, Privacy and Data Protection (CPDP 2022), Measuring Fundamental Rights Compliance through criminal justice statistics, OCTOPUS
- 25-26 May, C-PROC/MAURITIUS, *(hybrid),* Series of workshops on the new cybercrime legislation and Budapest Convention, GLACY+
- 25-27 May, C-PROC/NORTH MACEDONIA, *(in person),* Training Course on Financial Investigations, Virtual Currencies and Darknet, iPROCEEDS-2
- 27 May, C-PROC/GEORGIA, *(in person),* Forum of criminal justice, civil society and private sector on transparency of cybercrime action, CyberEast
- 27 May, C-PROC/MAURITIUS, *(in person),* Advisory mission on LEA training strategies, GLACY+
- 30-31 May, C-PROC/BRAZIL, *(online),* Series of webinars on Budapest Convention and cybercrime legislation, GLACY+
- 30 May-1 June, C-PROC/GHANA, *(in person),* Advisory mission on search, seizure, and confiscation of online proceeds of crime, GLACY+
- 30 May-10 June, C-PROC/AUSTRIA, *(hybrid),* UN Ad Hoc Committee 2nd meeting on new UN Treaty, GLACY+, iPROCEEDS-2, CyberSouth, OCTOPUS
- 31 May-3 June, C-PROC/SENEGAL, *(hybrid),* Support for the national delivery on the Introductory course on cybercrime and electronic evidence (jointly organized with OCWAR-C), GLACY+
- May-June, C-PROC, *(online),* Update of the 2018 Study on Cybercrime Threats and Strategies in the EaP region, CyberEast
- 30 May-3 June, C-PROC/CEPOL (*online*), CEPOL, Cross-border exchange of 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