Cybercrime Digest

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

15 – 30 June 2022

Source: US Department of Justice

Date: 16 June 2022

United States and EU Foster Cooperation Against Ransomware Attacks

"Ransomware has become a global problem that requires cooperation on a worldwide level. Judicial experts and practitioners from the United States and the European Union participated in a two-day workshop in The Hague organized by the U.S. Department of Justice and Eurojust. The event aimed to share best practices and enhance collaboration in confronting ransomware attacks. The event was opened by Eurojust President Ladislav Hamran and Assistant Attorney General Kenneth A. Polite, Jr. of the U.S. Department of Justice's Criminal Division. […] Assistant Attorney General Polite said: "Only by working together with key law enforcement and prosecutorial, partners in the EU can we effectively combat the threat that ransomware poses to our society. I am confident that the U.S.-EU ransomware workshop will spur greater coordination and collaboration to address the ransomware threat." READ MORE

Source: Euractiv

Date: 29 June 2022

EU co-legislators agree on 'key elements' of electronic evidence package

"The EU Parliament, Council and Commission have bridged their differences on several fundamental points regarding accessing cross-border electronic evidence, but some political issues remain. The e-Evidence package is intended to facilitate access to electronic communications across EU countries in the context of criminal investigations. As a result, law enforcement agencies could request access to evidence directly from the service provider in the other member state or even ask that the data be retained." READ MORE

RELATED ARTICLE:

S&D, E-evidence will bring a major paradigm shift in police, justice and service provider cooperation in the EU, 28 June 2022

Source: Microsoft

Date: 22 June 2022

Defending Ukraine: Early Lessons from the Cyber War

"[…] The Russian invasion relies in part on a cyber strategy that includes at least three distinct and sometimes coordinated efforts – destructive cyberattacks within Ukraine, network penetration and espionage outside Ukraine, and cyber influence operations targeting people around the world. […] The cyber aspects of the current war extend far beyond Ukraine and reflect the unique nature of cyberspace. When countries send code into battle, their weapons move at the speed of light. The internet's global pathways mean that cyber activities erase much of the longstanding protection provided by borders, walls, and oceans. And the internet itself, unlike land, sea, and the air, is a human creation that relies on a combination of public and private- sector ownership, operation, and protection." READ MORE

RELATED REPORT:

Microsoft, Defending Ukraine: Early Lessons from the Cyber War, 22 June 2022

Source: Council of Europe

Date: 30 June 2022

Côté d'Ivoire invited to join the Convention on Cybercrime

"Côté d'Ivoire was invited on 30 June 2022 to accede to the Budapest Convention on Cybercrime. Thus, 82 States are now either Parties (66), or have signed it or been invited to accede (16). The authorities of Côté d'Ivoire have been cooperating with the Council of Europe in cybercrime matters on multiple occasions since 2011." READ MORE

Source: OCCRP

Date: 23 June 2022

Critics Say Russia Wants UN Cyber Treaty to Harm Rights, Protect Criminals

"As talks on a U.N. cybercrime treaty gather pace, some accuse Russia of trying to forge cover for human rights abuses and criminal groups staging attacks against the West. OCCRP spoke with cybersecurity experts and a source privy to the ongoing negotiations, coordinated by the UN Office on Drugs and Crime, on an envisioned convention for countering use of ICT technologies for criminal purposes. They suggested Moscow has styled itself an "honest broker" on cybersecurity issues to win support from developing countries, pushing for provisions that would further enable suppression of dissent at home and widen the way for cybercriminal groups to pursue attacks against unfriendly states." READ MORE

Source: Council of Europe

Date: 28 June 2022

Council of Europe Digital Partnership: two new partners

"The International Chamber of Commerce and The LEGO Group have joined the Council of Europe's Digital Partnership, an initiative aimed at fostering cooperation with companies and their business associations to promote respect for human rights, democracy and the rule of law on the internet. During a signing ceremony in Strasbourg, Secretary General Marija Pejčinović Burić exchanged letters formalising their collaboration in the partnership with Andrew Wilson, Global Policy Director of the International Chamber of Commerce; and Edward Lewin, Vice-President of Government and Public Affairs of The LEGO Group." READ MORE

Source: Europol

Date: 23 June 2022

Human traffickers luring Ukrainian refugees on the web targeted in EU-wide hackathon

"On 23 May 2022, an EMPACT coordinated online joint action day targeted criminal networks grooming Ukrainian refugees for sexual and labour exploitation via websites and social media platforms. Law enforcement authorities from 14 EU Member States took part in this hackathon, coordinated by the Netherlands. […] The monitoring activities led to the identification of new trends and gathered insights into the threat of sexual and labour exploitation of Ukrainian refugees. Suspicious activities were detected in a wide range of platforms, including in the Russian language. Different platforms were prioritised depending on the specific social media use per country." READ MORE

Source: Interpol

Date: 15 June 2022

Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams

"A worldwide crackdown on social engineering fraud has seen scammers identified globally, substantial criminal assets seized and new investigative leads triggered in every continent. The two-month (8 March – 8 May 2022) Operation, codenamed First Light 2022, saw 76 countries take part in an international clampdown on the organized crime groups behind telecommunications and social engineering scams. Although results are still coming in, preliminary figures reached so far include: 1,770 locations raided worldwide; some 3,000 suspects identified; some 2,000 operators, fraudsters and money launderers arrested; some 4,000 bank accounts frozen; some USD 50 million worth of illicit funds intercepted." READ MORE

Source: Agencia de Informacion Paraguaya

Date: 20 June 2022

Paraguay ratificó su compromiso en la lucha contra el uso de las TIC con fines delictivos

"La delegación paraguaya que participó en Viena del segundo periodo de sesiones del Comité Intergubernamental Especial de Composición Abierta ratificó la convicción del Gobierno Nacional y su compromiso en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. […] Entre otros puntos, la delegación paraguaya resaltó la necesidad de armonizar esta nueva convención con los instrumentos internacionales ya existentes, como el Convenio de Budapest del cual Paraguay es parte, y los esfuerzos a nivel nacional, regional e internacional para combatir los delitos cibernéticos." READ MORE

Source: Comercio y Jusicia

Date: 24 June 2022

Chile aprobó una ley que sanciona los delitos informáticos

"Por unanimidad, la Cámara de Diputados de Chile modernizó la ley de delitos informáticos que, entre otras, adecúa figuras a la Convención de Budapest, como defraudación informática o el acceso indebido a sistemas o datos, y agrega nuevos tipos. La ley 21459, que deroga la ley N° 19223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, se publicó recientemente en el Boletín Oficial." READ MORE

Source: La Diaria Justicia

Date: 28 June 2022

Uruguay: Ciberdelitos: legisladores buscan avanzar en tres proyectos complementarios

"[…] Tras recibir los aportes del Consejo Europeo, la cancillería y la Fiscalía General de la Nación, los legisladores de la Comisión Especial de Innovación, Ciencia y Tecnología analizan avanzar en tres proyectos complementarios sobre ciberseguridad: uno que tipifique los nuevos delitos, otro relacionado a los procedimientos operativos en la investigación penal y otro que establezca los parámetros para la cooperación internacional." READ MORE

Source: INTERPOL

Date: 28 June 2022

Transnational crime threats faced by Africa focus of INTERPOL meeting

"From human and drug trafficking to terrorism and cybercrime, the range of security challenges faced by Africa is the focus of the INTERPOL African Regional Conference. Bringing together some 120 senior police officials from 29 countries, the meeting will also hear how cooperation between INTERPOL and regional bodies, including the African Union, CAPCCO, EAPCCO and WAPCCO, is delivering strong results. Officially opening the meeting, Benin's Minister of Interior and Public Security Alassane Seidou said, "[…] Hosting this conference demonstrates Benin's commitment to fighting transnational organized crime, including terrorism, through enhanced regional and international cooperation." READ MORE

Source: MISA

Date: 16 June 2022

Zimbabwe: Here's your citizen's guide to the Cyber Security & Data Protection Act

"The Media Institute of Southern Africa (MISA) Zimbabwe has today unveiled a guide to the Cyber Security and Data Protection Act. This outline is there so that ordinary Zimbabweans will be able to understand what the new act entails. This Guide intends to assist ordinary citizens, data protection advocates, human rights advocates, media organisations and interested individuals in getting a basic understanding and application of the Cyber and Data Protection Act." READ MORE

Source: InforPress

Date: 20 June 2022

Cape Verde: Profissionais participam em workshop consultivo sobre racionalização dos procedimentos para assistência jurídica mútua

"Os profissionais que trabalham com o cibercrime, participam, a partir de hoje, na Cidade da Praia, num workshop consultivo sobre a racionalização dos procedimentos para a assistência jurídica mútua relacionada com o cibercrime e a prova electrónica. Implementado pelo Conselho da Europa e financiado pela União Europeia, enquadrado nas actividades de capacitação do Projecto Glacy Plus, beneficiam do workshop que arrancou hoje, 20 e termina 24 de Junho, os Magistrados Judiciais, Procuradores da República e Inspectores da Polícia Judiciária que trabalham com a matéria do cibercrime." READ MORE

RELATED ARTICLES:

Council of Europe, GLACY+: Workshop to streamline procedures for mutual legal assistance in Cape Verde, 21 June 2022

TIVER, Racionalização Dos Procedimentos Para Assistência Jurídica Mútua, 20 June 2022

Council of Europe, GLACY+: Specialised Course on International Cooperation for Prosecutors and Judges in Cape Verde, 24 June 2022

Source: Council of Europe

Date: 24 June 2022

GLACY+: Petty Officers Gendarmerie of Senegal attended the First Responders Training of Trainers

"Under the framework of the GLACY+ Project, around 30 petty officers of the Gendarmerie of Senegal benefited from a First Responders Training of Trainers […]. The training was organized in cooperation with the Gendarmerie of Senegal and with the assistance of the French Gendarmerie. The training focused on equipping petty officers with the knowledge and skills on handling cybercrime-related scenes or crime scenes containing electronic evidence whose integrity must be preserved." READ MORE

Source: Council of Europe

Date: 28 June 2022

CyberSouth: National Workshop on the application of the Second Addition Protocol to the Budapest Convention for Lebanese authorities

"On 28 June 2022, the Cybercrime Programme Office of the Council of Europe (C-PROC), within the framework of the CyberSouth project and in cooperation with the Lebanese Ministry of Justice, organised a National Workshop on the Second Addition Protocol to the Budapest Convention on enhanced co-operation and the disclosure of electronic evidence." READ MORE

RELATED ARTICLE:

Council of Europe, CyberSouth: National Workshop on the application of the Second Additional Protocol to Budapest Convention, organised for Algerian authorities, 21 June 2022

Source: The Register

Date: 22 June 2022

Israeli air raid sirens triggered in possible cyberattack

"Air raid sirens sounded for over an hour in parts of Jerusalem and southern Israel on Sunday evening – but bombs never fell […]. While the perpetrator remains unclear, Israel's National Cyber Directorate did say in a tweet that it suspected a cyberattack because the air raid sirens activated were municipality-owned public address systems, not Israel Defense Force alarms as originally believed." READ MORE

Source: Cyber Scoop

Date: 27 June 2022

Iranian steel facilities suffer apparent cyberattacks

"Three Iranian steel companies suffered apparent cyberattacks Monday, claimed a hacktivist group that previously took responsibility for a digital assault on the Iranian train system with wiper malware. […] A hacktivist group calling itself "Gonjeshke Darande" claimed responsibility for the attacks in messages posted to its Telegram channel and on Twitter. The group posted screenshots purportedly showing the inside of one of the steel facilities and what appears to be an industrial control dashboard." READ MORE

Source: WIRED

Date: 15 June 2022

Russia Is Taking Over Ukraine's Internet

"Web pages in the city of Kherson in south Ukraine stopped loading on people's devices at 2:43 pm on May 30. […] They were stuck in a communications blackout. When web pages started stuttering back to life at 3:42 pm, everything appeared to be normal. But behind the scenes everything had changed: Now all internet traffic was passing through a Russian provider and Vladimir Putin's powerful online censorship machine." READ MORE

Source: Bleeping Computer

Date: 29 June 2022

Ukraine arrests cybercrime gang operating over 400 phishing sites

"The Ukrainian cyberpolice force arrested nine members of a criminal group that operated over 400 phishing websites crafted to appear like legitimate EU portals offering financial assistance to Ukrainians. The threat actors used forms on the site to steal visitors' payment card data and online banking account credentials and perform fraudulent, unauthorized transactions like moving funds to accounts under their control." READ MORE

Source: Hackread

Date: 21 June 2022

President Putin's Economic Forum Speech Delayed due to DDoS Attack

"The Russian Economic Forum was taking place in St. Petersburg when its proceedings were stalled due to a DDoS attack. A Distributed Denial of Service attack disrupted the proceedings at the 25th St Petersburg International Economic Forum, regarded as the Russian answer to the Davos World Economic Forum. The incident occurred on Friday. As a result, the speech of Russian premier Vladimir Putin got delayed for around 100 minutes at the country's flagship forum. Putin had to start his speech more than an hour after its scheduled start time." READ MORE

Source: Europol

Date: 21 June 2022

Phishing gang behind several million euros worth of losses busted in Belgium and the Netherlands

"A cross-border operation, supported by Europol and involving the Belgian Police (Police Fédérale/Federale Politie) and the Dutch Police (Politie), resulted in the dismantling of an organised crime group involved in phishing, fraud, scams and money laundering." READ MORE

Source: Bleepingcomputer

Date: 23 June 2022

Lithuania warns of rise in DDoS attacks against government sites

"The National Cyber Security Center (NKSC) of Lithuania has issued a public warning about a steep increase in distributed denial of service (DDoS) attacks directed against public authorities in the country. […] According to NKSC, due to these cyberattacks, Lithuania's transportation agencies, financial institutions, and other large entities have experienced temporary service disruptions." READ MORE

Source: The Hill

Date: 28 June 2022

Norway hit with cyberattack, temporarily suspending service

"Norway's public and private sector websites were temporarily down on Wednesday following a cyberattack that targeted the country's national data network, forcing it to suspend online services for several hours. […] The attack on Norway comes two days after Lithuania reported a similar hack that targeted public and private institution websites." READ MORE

Source: Council of Europe

Date: 15 June 2022

iPROCEEDS-2: Strengthening Criminal Justice Authorities and ISP Cooperation in Kosovo[1]

"[…] The Cybercrime Programme Office (C-PROC), and the iPROCEEDS-2 project, a joint action of the European Union and the Council of Europe, supported Kosovo[1] judicial authorities to strengthen their cooperation with the private sector, specifically with local Internet Service Providers (ISPs), by organising a specific conference in Pristina, Kosovo[1]." READ MORE

Source: Italy24 News

Date: 25 June 2022

Hacker attack on the Sardinia Region, personal data on the dark web

"The Autonomous Region has received notice of the publication on the dark web of folders containing personal data of its employees and users of some General Directions. The contents of the information are available on the dark web. […] The publication appears to be linked to a cyber-attack suffered by the administration in early February […]." READ MORE

Source: TechCrunch

Date: 29 June 2022

UK urgently needs new laws on use of biometrics, warns review

"An independent review of UK legislation has concluded the country urgently needs new laws to govern the use of biometric technologies and called for the government to come forward with primary legislation. Among the legal review's ten recommendations are that public use of live facial recognition (LFR) technology be suspended pending the creation of a legally binding code of practice governing its use, and pending the passing of wider, technologically neutral legislation to create a statutory framework governing the use of biometrics against members of the public." READ MORE

Source: Malwarebytes Labs

Date: 20 June 2022

DDoS-for-hire service provider jailed

"Matthew Gatrel, a 33-year-old man from St. Charles, Illinois, has been sentenced to two years in prison for running websites that provide powerful distributed denial-of-service (DDoS) attacks against internet users and websites. […] Gatrel's services helped launch attacks against targets worldwide, including homes, schools, universities, financial institutions, and local government websites." READ MORE

[1] This designation is without prejudice to positions on status and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo* Declaration of Independence.

Source: The Register

Date: 21 June 2022

Info on 1.5m people stolen from US bank in cyberattack

"In a statement to the office of Maine's Attorney General this month, Flagstar Bank said it was compromised between December and April 2021. The organization's sysadmins, however, said they hadn't fully figured out whose data had been stolen, and what had been taken, until now. On June 2, they concluded criminals "accessed and/or acquired" files containing personal information on 1,547,169 people." READ MORE

Source: The Globe and Mail

Date: 28 June 2022

Canada: New cybersecurity bill needs to be backed by resources

"Public Safety Minister Marco Mendicino recently tabled legislation that would mandate that businesses in four federally-regulated industries report cyberbreaches. It makes sense for the government to try to tackle this growing global challenge given that it's estimated that an attack occurs ever 11 seconds and the cost of cybercrime to the global economy will top US$10.5 trillion annually by 2025. However, without wider applicability and a thoughtful implementation strategy that includes training and technology solutions for police agencies, the legislation may do little to actually protect Canadians, especially the most vulnerable among us" READ MORE

Source: US Department of Justice

Date: 30 June 2022

Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving Over $100 Million in Intended Losses

"The Department of Justice, together with federal law enforcement partners, today announced criminal charges against six defendants in four separate cases for their alleged involvement in cryptocurrency-related fraud, including the largest known Non-Fungible Token (NFT) scheme charged to date, a fraudulent investment fund that purportedly traded on cryptocurrency exchanges, a global Ponzi scheme involving the sale of unregistered crypto securities, and a fraudulent initial coin offering." READ MORE

Latest reports

- Techeconomy, NCS Cybersecurity Forum Recommends over 15 Ways to Tackle Cybercrime, 15 June 2022
- Bleeping Computer, Citrix warns critical bug can let attackers reset admin passwords, 15 June 2022
- Hertzbleed.com, Hertzbleed Attack, 15 June 2022
- Sage Journals, Joanna Curtis, Gavin Oxburgh, Understanding cybercrime in 'real world' policing and law enforcement, 16 June 2022
- Mondaq, Saudi Arabia: Breaking Down Saudi Arabia's New Evidence Law, 16 June 2022
- Rapid7, New Report Shows What Data Is Most at Risk to (and Prized by) Ransomware Attackers, 16 June 2022
- The Daily Swig, Attackers can use 'Scroll to Text Fragment' web browser feature to steal data – research, 20 June 2022
- Malwarebytes Lab, Client-side Magecart attacks still around, but more covert, 20 June 2022
- Talos, Avos ransomware group expands with new attack arsenal, 21 June 2022
- ProofPoint, How Threat Actors Hijack Attention: The 2022 Social Engineering Report, 22 June 2022
- CISA, CISA Releases Security Advisories Related to OT:ICEFALL (Insecure by Design) Report, 22 June 2022
- Medianama, Deep Dive: What's Wrong With India's E-Commerce Rules And How Can They Be Fixed?, 23 June 2022
- Google, Spyware vendor targets users in Italy and Kazakhstan, 23 June 2022
- ENISA, The Annual Privacy Forum (APF) celebrates its first 10 years, as the links between privacy protection & cybersecurity continue to grow, 24 June 2022
- Talos, De-anonymizing ransomware domains on the dark web, 28 June 2022
- GoSecure, Did You Know Your Browser's Autofill Credentials Could Be Stolen via Cross-Site Scripting (XSS), 29 June 2022
- Lumen, ZuoRAT Hijacks SOHO Routers To Silently Stalk Networks, 28 June 2022
- EUROJUST, Cybercrime Judicial Monitor – Issue 7, 30 June 2022
- PIXM, Phishing tactics: how a threat actor stole 1M credentials in 4 months, June 2022
- Digital Citizens Alliance, How website retailers enable bad actors to become the master of illicit domains, June 2022
- Proof Point, How Threat Actors Hijack Attention: The 2022 Social Engineering Report, June 2022

Upcoming events

- 4-6 July, C-PROC/INTERPOL/PHILIPPINES, (*in-person*), Advisory mission on search, seizure, and confiscation of online proceeds of crime, GLACY+
- 4-7 July, C-PROC/SENEGAL, (*in-person*), Support for the national delivery/Introductory course on cybercrime and electronic evidence (in cooperation with OCWAR-C project), GLACY+
- 4-8 July, C-PROC/CEPOL/ROMANIA, *(in person),* Regional workshop on interagency and international cooperation on cyber-attacks, iPROCEEDS-2
- 11-14 July, C-PROC/ USA DoJ/TURKIYE, *(in person),* International mock trial on ransomware investigation, iPROCEEDS-2
- 12 July, C-PROC, (*online*), Ad-Hoc Working group on development of a guide on judicial training strategies on cybercrime and electronic evidence, GLACY+
- 12-14 July, C-PROC/SERBIA, *(in person),* Training skill certification programme for judges and prosecutors delivering Council of Europe judicial training on cybercrime and electronic evidence, iPROCEEDS-2
- 13 July, C-PROC, (*online*), GLACY+ 12th Steering Committee, GLACY+
- 13-15 July, C-PROC/LEBANON, (*in-person*), Judicial Training on International Cooperation, CyberSouth
- 14 July, C-PROC/LEBANON, (*in-person*), Meeting with the national ICT committee, CyberSouth
- July 2022, C-PROC/EAP Region, *(online),* Guidelines on the prevention and control of online fraud and criminal money flows, CyberEast
- July/August 2022, C-PROC/EAP Region, *(online),* Regional Study on legislation concerning search, seizure and confiscation of cybercrime proceeds and prevention of money laundering on the Internet in line with data protection requirements, CyberEast

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