Cybercrime Digest

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

1 – 15 January 2023

Source: Council of Europe

Date: 03 Jan 2023

The global state of cybercrime legislation as at January 2023!

"Countries around the globe keep improving their domestic criminal law in line with the Budapest Convention on Cybercrime. An updated cursory overview of the "Global State of Cybercrime Legislation" prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC) indicates that by 1 January 2023, some 130 States (67% of UN members) were considered to have criminalized offences against and by means of computers largely in line with the Convention on Cybercrime." READ MORE

Source: Axios

Date: 10 Jan 2023

The UN is trying to define cybercrime

"Over the next two weeks, a group of nations is trying to answer one of the most basic questions in cybersecurity: What exactly is considered cybercrime? […] The current treaty negotiations have faced political strife from the very beginning, when the Russian delegation requested the UN create such a pact in the first place. […] Many human rights groups argue the cybercrime treaty isn't needed since the 2001 Budapest Convention covers many of these issues already." READ MORE

RELATED ARTICLE:

Ifex, UN Cybercrime Convention must be revised to include human rights safeguards, 9 January 2023

Cybernews, UN cybercrime treaty to boost international cooperation or increase surveillance? Experts are divided, 12 January 2023

Source: Council of Europe

Date: 10 Jan 2023

UN AHC side event – the Convention on Cybercrime in practice: lessons learnt 2001 – 2022 (Vienna, 10 January 2023)

"As the members of the United Nations are engaged in a process of negotiating a new international treaty on "Countering the Use of Information and Communications Technologies for Criminal Purposes", they may draw on lessons learnt from the experience of the Convention on Cybercrime over more than twenty years since it was opened for signature in Budapest in 2001." READ MORE

Source: European Parliament

Date: 12 Jan 2023

MEPs back international agreement on sharing electronic evidence

"On Thursday, MEPs gave their backing to the ratification of the Additional Protocol to the Council of Europe's Budapest Convention on Cybercrime. MEPs on the Civil Liberties Committee have endorsed the ratification of the Second Additional Protocol to the Budapest Convention on Cybercrime, an international agreement aiming to smoothen co-operation in fighting cybercriminality." READ MORE

Source: Politico

Date: 09 Jan 2023

Kyiv argues Russian cyberattacks could be war crimes

“One of Ukraine's top cyber officials said some cyberattacks on Ukrainian critical and civilian infrastructure could amount to war crimes. Victor Zhora, chief digital transformation officer at the State Service of Special Communication and Information Protection (SSSCIP) of Ukraine, said Russia has launched cyberattacks in coordination with kinetic military attacks as part of its invasion of Ukraine, arguing the digital warfare is part of what Kyiv considers war crimes committed against its citizens. […] “Ukrainian officials are gathering evidence of cyberattacks linked to military strikes and are sharing the information with the International Criminal Court (ICC) in the Hague, in an effort to support potential prosecutions into Russia's actions, Zhora said.” READ MORE

RELATED ARTICLES:

Eureporter, Ukraine war and geopolitics fuelling cybersecurity attacks - EU agency, 9 January 2023

The Record, Poland warns of pro-Kremlin cyberattacks aimed at destabilization, 31 December 2022

Source: CircleID

Date: 11 Jan 2023

C NIS, IC2, ICANN and Thick WHOIS: A Mandate to Move Forward

“The recent adoption at the end of December of the new EU Directive for a high level of cybersecurity across the Union—commonly referred to as “NIS2”—paved the way for important updates to the domain name system (DNS). Most significantly, Article 28 of NIS2 and its related recitals resolved any ambiguities about the public interest served by a robust and objectively accurate WHOIS system that permits legitimate access by third parties to data, including personal data, and the legal basis under the EU General Data Protection Regulation (“GDPR”) that supports such a system. ” READ MORE

Source: US Department of Justice

Date: 12 Jan 2023

Crypto Fraud Victims Receive Over $17 Million in Restitution from BitConnect Scheme

“A federal district court in San Diego ordered today that over $17 million in restitution be distributed to approximately 800 victims from over 40 different countries due to their investment losses in BitConnect, a massive cryptocurrency investment scheme, which defrauded thousands of investors worldwide.” READ MORE

Source: Security Affairs

Date: 05 Jan 2023

Data of 235 million Twitter users leaked online

“A data leak containing email addresses for 235 million Twitter users has been published on a popular hacker forum. Many experts have immediately analyzed it and confirmed the authenticity of many of the entries in the huge leaked archive. […] The seller, who is a member of a popular data breach forum, claimed the data was scraped via a vulnerability. The database includes emails and phone numbers of celebrities, politicians, companies, normal users, and a lot of OG and special usernames.” READ MORE

Source: Council of Europe

Date: 13 Jan 2023

Capacity building on cybercrime: New report on the activities of C-PROC

"Between October 2021 and December 2022, the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania supported some 420 capacity building activities on cybercrime and electronic evidence involving over 130 countries. The report on C-PROC, that the Secretary General just shared with the Committee of Ministers of the Council of Europe, shows that important impact was achieved worldwide in this period in spite of a challenging context that included in particular the Russian aggression against Ukraine." READ MORE

RELATED REPORT:

Council of Europe, Capacity building on cybercrime: New report on the activities of C-PROC, 13 January 2023

Source: Eurojust

Date: 12 Jan 2023

Takedown of fraudulent cryptocurrency network in Bulgaria, Cyprus and Serbia

"With the active support of Eurojust and Europol, a coordinated action has led to the dismantling of a cryptocurrency fraud network operating from Bulgaria, Cyprus and Serbia. The network operated professionally to set up call centres, which defrauded numerous victims in Germany, Switzerland, Austria, Australia and Canada for at least tens of millions of euros. […] Overall, more than 250 persons were interviewed and over 150 computers, various electronic equipment and data back-ups, three cars, two luxury apartments and one million US dollars in cryptocurrencies and 50 000 EUR in cash were seized." READ MORE

Source: Graham Cluley

Date: 03 Jan 2023

Data of over 200 million Deezer users stolen, leaks on hacking forum

"Music-streaming service Deezer has owned up to a data breach, after hackers managed to steal the data of over 200 million of its users. […] According to RestorePrivacy which first reported on the breach, the hacker released a sample 5 million stolen records on a well-known hacking forum, claiming to have a 60GB stash of stolen data, including 228 million email addresses. READ MORE

Source: Gulf Business

Date: 11 Jan 2023

Cybersecurity 2023: Threats proliferate but best practice still works

"The year 2022 has been unrelenting on the cybersecurity front and adversaries are only becoming more sophisticated and adopting more advanced techniques and technologies to circumvent organisations' security measures. Ransomware has remained the most dangerous, costly and prevalent cyberthreat to EMEA organisations last year, and will continue to be the most damaging cybercrime tool of 2023." READ MORE

Source: Check Point Research

Date: 05 Jan 2023

Blindeagle targeting Ecuador with sharpened tools

"APT-C-36, also known as Blind Eagle, is a financially motivated threat group that has been launching indiscriminate attacks against citizens of various countries in South America since at least 2018. In a recent campaign targeting Ecuador based organizations, CPR detected a new infection chain that involves a more advanced toolset. […] One typical example is an email purportedly from the Ministry of Foreign Affairs, threatening the recipient with issues when leaving the country unless they settle a bureaucratic matter. READ MORE

Source: Nacional

Date: 10 Jan 2023

Peru: Fiscalía resuelve el 58 % de casos de ciberdelincuencia los últimos 6 meses del 2022

La Fiscalía especializada en Ciberdelincuencia de Lima Centro logró resolver el 58 % de los casos ingresados en el segundo semestre del 2022 y durante ese periodo fueron recibidas 5,370 denuncias referidas a delitos informáticos. De esta manera, se presenta una diferencia con relación al periodo del 15 de junio del 2021 a julio del 2022, que ingresaron 10 169 casos, resolviéndose 5108 de ellos; lo cual evidencia un avance del 50.2 % de la carga READ MORE

Source: Leaders

Date: 10 Jan 2023

Tunisie: Modernité et complétude de la législation relative à la cybersécurité et à la cybercriminalité: Un édifice en 10 étages

"L'obsolescence des textes régissant le domaine de la cybersécurité et le vide juridique relatif à la lutte contre la cybercriminalité étaient parmi les principales préoccupations du ministre des Technologies de la communication. Ces lacunes représentaient des obstacles majeurs face à la mise en œuvre effective de la stratégie nationale de cybersécurité et de lutte contre la cybercriminalité. Nizar Ben Neji, lui-même expert en cybersécurité, a réussi avec son équipe à élaborer le projet du décret-loi relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication. Ce nouveau texte, promulgué au mois de septembre 2022, aura un véritable effet dissuasif sur les crimes cybernétiques en Tunisie." READ MORE

Source: Africa Center

Date: 03 Jan 2023

Learning from Ghana's Multistakeholder Approach to Cyber Security

"As internet penetration has exponentially grown, African countries have become more exposed to cyber-related threats. Most African countries have experienced at least one publicly documented disinformation campaign, a majority of which are sponsored by external actors. […] Ghana is not most African countries. It is 1 of only 12 nations in Africa to possess both a national cybersecurity strategy and national incident response capabilities. It is also one of only four to have ratified both the Budapest and Malabo Conventions, two major treaties aimed at addressing the international dimensions of cyber-related threats. READ MORE

Source: The Diplomat

Date: 05 Jan 2023

Ransomware: A Wake-Up Call for Cybersecurity in the Indo-Pacific

“The 2021 report by cybersecurity firm Sophos found that 78 percent of Indian firms were targeted by ransomware attacks, signifying the rising level of such crimes. Similar trends are visible across the Indo-Pacific, with countries in the region among the most targeted by ransomware attacks in the previous year. […] The recent ransomware attack on AIIMS, one of the largest public health institutions in India, highlighted the dangers cyberattacks can pose to human life. Attackers targeted AIIMS servers with malware that made the servers dysfunctional.” READ MORE

Source: The Hacker News

Date: 11 Jan 2023

Australian Healthcare Sector Targeted in Latest Gootkit Malware Attacks

“A recent wave of Gootkit malware loader attacks has targeted the Australian healthcare sector by leveraging legitimate tools like VLC Media Player. Gootkit, also called Gootloader, is known to employ search engine optimization (SEO) poisoning tactics (aka spamdexing) for initial access. It typically works by compromising and abusing legitimate infrastructure and seeding those sites with common keywords.” READ MORE

Source: Euractiv

Date: 10 Jan 2023

Tech Brief: Germany`s AI reservations, fair share moves in the metaverse

At the Telecom Council in December, German digital minister Volker Wissing made clear Berlin still has some reservations about the AI Act, which it hopes will be solved at the trilogue stage. The more recent documents also include some additional points, for instance, the mention that “as it stands now, providers of general purpose AI systems may face a variety of issues that result in investment and innovation attentisms.” READ MORE

Source: Euronews

Date: 11 Jan 2023

Hackers hit websites of Danish central bank, other banks

“Hackers have disrupted access to the websites of Denmark’s central bank and seven private banks in the country this week, according to the central bank and an IT firm that serves the industry. The websites of the central bank and Bankdata, a company that develops IT solutions for the financial industry, were hit by so-called distributed denials of service (DDoS), which direct traffic towards targeted servers in a bid to knock them offline.” READ MORE

Source: BBC

Date: 13 Jan 2023

Royal Mail hit by Russia-linked ransomware attack

“Severe disruption to Royal Mail's overseas deliveries has been caused by ransomware linked to Russian criminals, the BBC has been told. The cyber-attack has affected the computer systems Royal Mail uses to despatch deliveries abroad. Royal Mail has been warning customers since Wednesday of disruption due to a "cyber-incident".” READ MORE

Source: The Record

Date: 09 Jan 2023

Serbian government reports 'massive DDoS attack' amid heightened tensions in Balkans

"The Serbian government announced on Saturday that the website and IT infrastructure of its Ministry of Internal Affairs had been hit by several "massive" distributed denial-of-service (DDoS) attacks. "So far five large attacks aimed at disabling the IT infrastructure of the Ministry of Interior have been repelled," said Belgrade, adding that government employees and staff from state-owned Telekom Srbija (Telecom Serbia) were able to counter the attacks." READ MORE

Source: The Hacker News

Date: 03 Jan 2023

Raspberry Robin Worm Evolves to Attack Financial and Insurance Sectors in Europe

"Financial and insurance sectors in Europe have been targeted by the Raspberry Robin worm, as the malware continues to evolve its post-exploitation capabilities while remaining under the radar. […] The intrusions, observed against Spanish and Portuguese-speaking organizations, are notable for collecting more victim machine data than previously documented, with the malware now exhibiting sophisticated techniques to resist analysis." READ MORE

Source: El Confidencial

Date: 9 Jan 2023

Spain: Nueve detenidos por distribuir pornografía infantil a través de una aplicación

"La Policía Nacional ha detenido en siete provincias a nueve personas, entre ellas dos menores de edad, acusadas de distribuir material de pornografía infantil a través de una aplicación de mensajería, informa este lunes la Dirección General del Cuerpo. La investigación ha contado con la colaboración de la Real Policía Montada de Canadá, Europol y el Centro Nacional de Coordinación de Explotación Infantil (NCECC)." READ MORE

Latest reports

- OECD, Declaration on Government Access to Personal Data held by Private Sector Entities, 14 December 2022
- Veracode, Annual Report on the State of Application Security, January 2023
- Electronic Frontier Fondation, Global Cybercrime and Government Access to Users Data Across Borders: 2022 in Review, 2 January 2023
- EMSISOFT, The State of Ransomware in the US: Report and Statistics 2022, 2 January 2023
- Council of Europe, Global State of Cybercrime Legislation, 3 January 2023
- Africa Center for Strategy Studies, Learning from Ghana`s Multistakeholder Approach to Cyber Security, 3 January 2023
- TrendMicro, The Evolution of Windows Kernel Threats, 5 January 2023
- Phylum, A Deep Dive Into poweRAT: a Newly Discovered Stealer/RAT Combo Polluting PyPI, 5 January 2023
- Bitdefender, Bitdefender Partnership with Law Enforcement Yields MegaCortex Decryptor, 5 January 2023
- Resecurity, Dark Web Markets Compete For The Drug Trafficking And Illegal Pharmacy Monopoly, 8 January 2023
- Finances Online, 16 Latest Cybercrime Trends & Predictions for 2022/2023 and Beyond, 9 January 2023
- IT Ware LATAM, Alarma: el ciberdelito se consolida como industria en 2023, 10 January 2023
-
- Research, Large language models will revolutionize digital propaganda campaigns, 11 January 2023
- Council of Europe, Capacity building on cybercrime: New report on the activities of C-PROC, 13 January 2023

Upcoming events

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime