Cybercrime Digest

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

16 - 31 January 2024

Source: The Record

Date: 23 January 2024

On eve of final negotiations, US says consensus growing around 'narrow' UN cybercrime treaty

"The U.S. government is holding firm in its desire for a much narrower version of a United Nations Cybercrime Treaty than the draft released in November, on the eve of a final round of negotiations later this month. Russia and several allies started the effort for the treaty in 2017, with the professed hopes of developing global rules addressing the thorny issue of transnational internet crimes." READ MORE

Source: ICC

Date: 22 January 2024

Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system

"Today, my Office was honoured to host an innovative conference addressing cyber-enabled crimes through the Rome Statute system. Gathering more than 100 participants including from 12 cybersecurity and technology companies at the International Criminal Court (ICC) in The Hague, this dialogue marks an important and concrete further step in exploring the less charted territories of cyber-enabled crimes within the context of international criminal law. As I stated in Foreign Policy last year, cyber-enabled crimes may fall within the ICC's jurisdiction if the requirements of the Rome Statute are met, and my Office may investigate or prosecute such conduct. One of our thematic priorities this year is to develop a policy setting out my Office's approach to this emerging issue, building on our engagement with all relevant partners." READ MORE

Source: Eurojust

Date: 22 January 2024

Crackdown on criminal network dealing with online investment fraud

"Judicial and law enforcement authorities in Germany, Cyprus, Bulgaria and Sweden have carried out a coordinated action against an organised crime group suspected of online trading fraud. The network defrauded numerous victims for several millions of euros in Germany and other European countries. During a joint action day supported by Eurojust and Europol, four suspects were arrested and thirteen places were searched." READ MORE

Source: INTERPOL

Date: 18 January 2024

Grooming, radicalization and cyber-attacks: INTERPOL warns of 'Metacrime'

"A comprehensive analysis of the Metaverse's key challenges, threats and harms from a law enforcement perspective is outlined in a new INTERPOL White Paper published today. Contributing towards a secure-by-design Metaverse, the document identifies current and potential Metacrimes, such as grooming, radicalization and cyber-physical attacks against critical infrastructure, as well as theft of 3D virtual/cultural property, trespassing in private virtual spaces, and robbery from an avatar." READ MORE

Source: Africa Cybersecurity Magazine

Date: 24 January 2024

Au Bénin, les députés autorisent la ratification de la convention de Malabo et de Budapest sur la cybersécurité et la protection des données

"Les députés de la 9e législature du Bénin, réunis au palais des gouverneurs ce mardi 23 janvier 2024, ont donné leur autorisation au gouvernement pour ratifier deux conventions essentielles. L'une concerne la cybercriminalité, et l'autre sur la cybersécurité. Il s'agit de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo) et de la convention de Budapest sur la cybercriminalité." READ MORE

Source: US Department of Justice

Date: 31 January 2024

U.S. Government disrupts botnet people's Republic of China used to conceal hacking of critical infrastructure

"A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-sponsored hackers. The hackers, known to the private sector as "Volt Typhoon," used privately-owned SOHO routers infected with the "KV Botnet" malware to conceal the PRC origin of further hacking activities directed against U.S. and other foreign victims. These further hacking activities included a campaign targeting critical infrastructure organizations in the United States and elsewhere that was the subject of a May 2023 FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and foreign partner advisory. The same activity has been the subject of private sector partner advisories in May and December 2023, as well as an additional secure by design alert released today by CISA." READ MORE

Source: European Parliament

Date: 18 January 2024

Time to criminalise hate speech and hate crime under EU law

"The Council should adopt a decision to include hate speech and hate crime among criminal offences within the meaning of Article 83(1) TFEU (so-called "EU crimes") by the end of the current legislative term, Parliament says in the report adopted on Thursday with 397 votes in favour, 121 against, and 26 abstentions. These are crimes of a particularly serious nature with a cross-border dimension, for which Parliament and Council can establish minimum rules to define criminal offences and sanctions. […] MEPs seek to ensure universal protection for all, with a special focus on targeted persons and vulnerable groups and communities. Currently, member states' criminal laws deal with hate speech and hate crime in different ways, while EU-wide rules apply only when such crimes are committed based on race, skin colour, religion, descent or national or ethnic origin." READ MORE

RELATED ARTICLE:

European Parliament, European Parliament resolution of 17 January 2024 on virtual worlds – opportunities, risks and policy implications for the single market, 17 January 2024

Source: European Commission

Date: 31 January 2024

Digital Services Act: Commission launches Transparency Database Update with Dashboard

“Today, the European Commission has launched a new user interface of the DSA Transparency Database as well as a new interactive dashboard that makes it easy to access summarised information on statements of reasons submitted by providers of online platforms. The transparency database is a unique regulatory repository that collects online platforms’ statements of reasons, which they are mandated to provide under the Digital Services Act (DSA) to explain to users why access to content has been removed or restricted. The transparency database is a crucial transparency tool under the DSA which provides unparalleled access to data on online content moderation to the public.” READ MORE

Source: ICANN

Date: 17 January 2024

ICANN Launches RDRS, Releases First Metrics Report

“In November, the ICANN organization launched the Registration Data Request Service (RDRS), a new service that provides a more consistent and standardized format to handle requests for access to nonpublic registration data related to generic top-level domains (gTLDs). The RDRS is an important mechanism for ICANN-accredited registrars and those who have a legitimate interest in accessing nonpublic data, including law enforcement, intellectual property professionals, consumer protection advocates, cybersecurity professionals, and government officials.” READ MORE

RELATED ARTICLE:

Domain incite, Weak demand for private Whois data, ICANN data shows, 17 January 2024

Source: Yahoo finance

Date: 16 January 2024

Venezuela terminates petro cryptocurrency after 5 years

“Venezuela has officially pulled the plug on its Petro cryptocurrency, ending a five-year experiment that was marred by controversy and corruption. The Petro was launched in 2018 by President Nicolas Maduro as a means to bolster the nation's currency, the bolívar, amid a severe economic crisis. Backed by Venezuela's oil reserves, the token was met with skepticism and opposition from the start. Critics, including the country's opposition-controlled congress, deemed the Petro illegal and accused the government of exploiting the nation's oil wealth. In 2019, the United States sanctioned a Russian bank for its involvement in financing the Petro.” READ MORE

Source: BlackBerry

Date: 24 January 2024

Mexican banks and cryptocurrency platforms targeted with AllaKore RAT

“A financially motivated threat actor is targeting Mexican banks and cryptocurrency trading entities with custom packaged installers delivering a modified version of AllaKore RAT – an open-source remote access tool. Lures use Mexican Social Security Institute (IMSS) naming schemas and links to legitimate, benign documents during the installation process.” READ MORE

Source: Bleeping Computer

Date: 19 January 2024

Payoneer accounts in Argentina hacked in 2FA bypass attacks

"Numerous Payoneer users in Argentina report waking up to find that their 2FA-protected accounts were hacked and funds stolen after receiving SMS OTP codes while they were sleeping. Payoneer is a financial services platform providing online money transfer and digital payment services. It is popular in Argentina because it allows people to earn in foreign currencies while bypassing local banking regulations. Starting last weekend, many Payoneer users in Argentina, whose accounts were protected by two-factor authentication (2FA), reported suddenly losing access to their accounts or simply logging in to empty wallets, losing "years of work" worth in money ranging from $5,000 to $60,000." READ MORE

Source: NBC News

Date: 27 January 2024

Sextortion training materials found on TikTok, Instagram, Snapchat and YouTube, according to new report

"A form of cybercrime called "financial sextortion" is rapidly rising in North America and Australia, with a major portion driven by a non-organized cybercriminal group in West Africa who call themselves "Yahoo Boys," according to a new study from the Network Contagion Research Institute (NCRI). […] Yahoo Boys' tactics gained popularity among some as a way to get rich quickly in West Africa, where there are scant other means of earning income, according to a 2023 Atavist investigation. Popular songs referencing Yahoo Boys have lent the cybercriminal gangs cultural clout." READ MORE

Source: Times Kuweit

Date: 25 January 2024

Kuweit: New strategies to curb cybercrime, enhance online experience

"In a recent statement, the Communications and Information Technology Regulatory Authority (CITRA) announced that it would soon introduce a slew of measures designed to curb mobile phone frauds and other cybercrimes in the country. This follows a spate of instances where individuals and institutions were defrauded by cybercriminals using new and sophisticated technologies and techniques." READ MORE

Source: The Record

Date: 16 January 2024

Southeast Asian casino industry supercharging cyber fraud, UN says

"The expanding Southeast Asian casino industry has become the nexus of the region's criminal ecosystem, including its cyber fraud industry, and it is facilitating large-scale money laundering by organized crime networks, a new United Nations report reveals. The money laundering includes the proceeds from online scams like pig-butchering schemes, where scammers develop a relationship with a victim and lure them into making fraudulent investments. […] The use of casinos to launder organized crime proceeds in Southeast Asia is not necessarily new. As the report points out, multiple Philippines-based casinos helped to launder about $81 million believed stolen by North Korea's Lazarus hacking group from Bangladesh Bank." READ MORE

Source: Reuters

Date: 24 January 2024

Sri Lanka passes new law to regulate online content

“Sri Lanka's lawmakers on Wednesday passed a bill to regulate online content, the speaker of the parliament announced, a law which opposition politicians and activists allege will muzzle free speech. […] Last year, the United Nations human rights office (OHCHR) said the law "could potentially criminalise nearly all forms of legitimate expression" while New York-based Human Rights Watch (HRW) said it would "seriously threaten" the right to freedom of expression in the country.” READ MORE

Source: New Indian Express

Date: 19 January 2024

India: ‘Golden hour to report cybercrime is 2 hours’: Cyberabad Deputy Commissioner

“With an alarming rise in the number of financial cybercrime cases, Cyberabad Deputy Commissioner of Police Cyber Crime Shilpavalli K noted that the “golden hour” to report cybercrime is two hours. Although a number of victims report cybercrime cases, not many do so within the first two hours, which is a crucial window, the DCP specified. Shilpavalli told TNIE that the sooner a cybercrime case is flagged, the faster the police can take action.” READ MORE

Source: Data Breach

Date: 24 January 2024

North Korean Hackers Using AI in Advanced Cyberattacks

“South Korea's intelligence agency reported Wednesday that North Korean hackers are using generative AI technology to conduct sophisticated cyberattacks and identify hacking targets. An official from the National Intelligence Service said the agency is monitoring North Korea's use of generative AI in cyberwarfare efforts. "North Korean hackers are using generative AI to find hacking targets and technologies needed for hacking," the official told the Yonhap News Agency.” READ MORE

Source: OCCRP

Date: 23 January 2024

Vietnam Law Enforcement to Tackle Growing Cybercrime

“Vietnamese criminologists, investigators, judges, and prosecutors gathered last week to learn how to better combat cybercrime, which is on the rise in the country and might have globally achieved a market value in excess of the illicit drug economy. With the support of the United Nations Office on Drugs and Crime (UNODC), law enforcement professionals were trained in countering cyber-related offenses.” READ MORE

Source: Resecurity

Date: 22 January 2024

Cybercriminals Leaked Massive Volumes Of Stolen PII Data From Thailand In Dark Web

“Recently, the Criminal Court in Thailand issued an order to block the website 9near.org. This action was taken after the site threatened to disclose the personal information of 55 million Thai citizens, allegedly obtained from vaccine registration records. The court further declared that any other websites found distributing data from "9near.org" would also face blocking.” READ MORE

Source: The Diplomat

Date: 20 January 2024

Confronting Digital Authoritarian-ism Through Digital Democracy: Lessons From Taiwan

"China has a history of foreign information manipulation and influence operations targeting Taiwan, from economic to political and diplomatic pressure, to cyber and cognitive warfare, and increasingly sophisticated disinformation operations. In fact, the most recent dataset from the Varieties of Democracy and Digital Society Project tracking foreign government manipulation of social media and disinformation among 202 countries from 2000-2021 showed Taiwan as the country most targeted globally by foreign disinformation operations. Rather than succumb to malicious foreign manipulation and influence, Taiwan has sought to "promote co-creation from tensions and conflicts," in the words of Digital Minister Audrey Tang, through a whole of society approach to digital democracy." READ MORE

Source: The Guardian

Date: 28 January 2024

Australia: Shadowy world of ransomware-for-hire revealed by online account activity linked to the Medibank hack

"Experts have pieced together the online history of Aleksandr Gennadievich Ermakov to reveal his alleged cybercrime operations in the years leading up to the attack. […] The government has named 33-year-old Aleksandr Gennadievich Ermakov, a Russian citizen, IT worker and alleged cybercriminal, in new sanctions legislation in connection with the most damaging cyberattack on Australians in 2022." READ MORE

RELATED ARTICLE:

KrebsonSecurity, Who is Alleged Medibank Hacker Aleksandr Ermakov?, 26 January 2024

Source: Supreme Court, Republic of the Philippines

Date: 23 January 2024

Philippine Judiciary Joins Efforts to Combat Cybercrime

"In a historic meeting held today at the Dignitaries' Lounge of the Supreme Court in Ermita, Manila, the Philippine Judiciary received from the Council of Europe's (COE) Global Action on Cybercrime Enhanced (GLACY-e) program the post-event Report from the Philippine delegation who attended the ceremonies of the closing of the Global Action on Cybercrime Extended (GLACY+) project and launch of GLACY-e in December 2023. The meeting symbolizes the collaborative commitment of the COE and the Philippines to strengthen their efforts towards the fight against cybercrime. The GLACY-e program is a joint project of the COE and the European Union. […] Associate Justice Jose Midas P. Marquez, who serves as the GLACY-e National Coordinator, said that "as a designated capacity-building hub for the ASEAN Region under the GLACY-e, it is a must for us to come up with an approach to judicial trainings aimed at empowering not only the Philippines but all ASEAN countries to develop their own courses and to constitute a pool of local trainers that are able to implement them."" READ MORE

Source: European Council

Date: 31 January 2024

EU-Japan economic partnership agreement: EU and Japan sign protocol to include cross-border data flows

"On behalf of the EU, the Belgian Presidency of the Council has signed the protocol to include provisions on cross-border data flows in the agreement between the EU and Japan for an Economic Partnership. The protocol will provide greater legal certainty, ensuring that data flows between the EU and Japan will not be hampered by unjustified data localisation measures, and also ensuring the benefit from the free flow of data according to the EU and Japan's rules on data protection and the digital economy." READ MORE

Source: The Record

Date: 24 January 2024

Ukrainian hackers claim attack on Russian scientific research center

"Pro-Ukraine hackers have reportedly breached a Russian scientific research center, Ukraine's defense intelligence directorate (GUR) said. According to GUR's report on Wednesday, the hacker group called "BO Team" attacked the State Research Center on Space Hydrometeorology, also known as "Planeta," and destroyed its database and valuable equipment." READ MORE

Source: The Record

Date: 29 January 2024

Ukraine's prisoners of war agency hit by cyberattack

"The Ukrainian state agency overseeing the treatment of prisoners of war said on Monday that it had restored access to its website after being hit by a distributed denial-of-service (DDoS) attack over the weekend. The country's Coordination Headquarters for the Treatment of Prisoners of War works with families of military personnel who were captured or missing and negotiates prisoner exchanges and the return of bodies of fallen soldiers." READ MORE

Source: Bank Info Security

Date: 22 January 2024

Ransomware hit on Tietoevry causes IT outages across Sweden

"A ransomware attack that hit a data center run by Finnish IT software and services firm Tietoevry has led to widespread outages across Sweden. Healthcare, local and national government services, retail outlets and the country's largest cinema chain are among the organizations experiencing ongoing disruptions." READ MORE

Source: SentinelOne

Date: 17 January 2024

Poland to investigate use of Pegasus spyware by former government

"Poland established a parliamentary inquiry commission On Wednesday to investigate allegations of the former ruling party, Law and Justice (PiS), using Israeli-developed spyware Pegasus to monitor political opposition. Last year, Polish media reported that the government had employed spyware on at least three occasions to monitor on those considered a nuisance to the government." READ MORE

Source: Cryptopolitan

Date: 30 January 2024

German authorities seize record 50,000 bitcoins in major cybercrime crackdown

"German law enforcement agencies have temporarily seized around 50,000 Bitcoins, valued at approximately $2.17 billion. This action, conducted in mid-January 2024, represents the largest Bitcoin confiscation in the country's history. The operation showcases Germany's increasing efforts to tackle cybercrime and financial offenses related to digital currencies." READ MORE

Source: IBT Times

Date: 31 January 2024

UK takes the lead in tackling cyberbullying as online safety act gets royal assent

"British people are set to get some relief from fake news, cyberflashing and other non-trivial forms of online abuse as the UK government introduced new plans to criminalise them. The Department for Science, Innovation and Technology announced on January 31 that new offences are being introduced to criminalise cyberflashing and fake news. This part of the Online Safety Act which come into force from today." READ MORE

Source: Security Week

Date: 24 January 2024

Major US, UK Water Companies Hit by Ransomware

"Two major water companies, Veolia North America in the United States and Southern Water in the United Kingdom, have been targeted in ransomware attacks that resulted in data breaches. […] In a notice posted on its website, Veolia North America revealed that its Municipal Water division was hit by ransomware last week. […] No known ransomware group appears to have taken credit for the attack on Veolia. […] Across the pond, a ransomware group targeted Southern Water, which provides water services to 2.5 million customers and wastewater services to 4.7 million customers in the South of England. […] The water sector in the West has been increasingly targeted by malicious cyber actors. Hackers believed to be affiliated with the Iranian government last year targeted industrial control systems (ICS) at multiple water facilities in the United States. In Ireland, a cyberattack targeting the systems of a small utility caused significant disruption, leaving people without water for two days." READ MORE

Source: BBC News

Date: 23 January 2024

US regulator admits cyber-security lapse before rogue Bitcoin post

"The US financial regulator has confirmed a key security procedure on its X account had been suspended for six months when hackers made a fake post about Bitcoin in January. The cryptocurrency surged in value before the post was deleted. The Securities and Exchange Commission (SEC) did not have multi-factor authentication (MFA) in place when hackers gained access to the account. Cyber-security experts say it should be a wake-up call for other agencies." READ MORE

Source: The Guardian

Date: 17 January 2024

Revealed: US police prevented from viewing many online child sexual abuse reports, lawyers say

“Social media companies relying on artificial intelligence software to moderate their platforms are generating unviable reports on cases of child sexual abuse, preventing US police from seeing potential leads and delaying investigations of alleged predators, the Guardian can reveal. […] Social media companies, Meta included, use AI to detect and report suspicious material on their sites and employ human moderators to review some of the flagged content before sending it to law enforcement. However, US law enforcement agencies can only open AI-generated reports of child sexual abuse material (CSAM) by serving a search warrant to the company that sent them. Petitioning a judge for a warrant and waiting to receive one can add days or even weeks to the investigation process.” READ MORE

Source: itbusiness.ca

Date: 29 January 2024

Hearings on Canada’s proposed cybersecurity law begin

“Work on the second plank of the Liberal government’s cybersecurity and privacy strategy started Monday afternoon. That’s when the House of Commons Standing Committee on Public Safety and National Security opened hearings on Bill C-26, which amends legislation governing telecommunications companies and creates the Critical Cyber Systems Protection Act (CCSPA). “This legislation is among the most important safety and regulatory regimes of a generation,” says David Shipley, head of New Brunswick’s Beauceron Security and co-chair of the Canadian Chamber of Commerce’s cyber council.” READ MORE

Latest reports

- Sentinel One, The Rise of Drainer-as-a-Service | Understanding DaaS, 16 January 2024
- CISA, FBI, Known Indicators of Compromise Associated with Androxgh0st Malware, 16 January 2024
- AXIOS, Exclusive: Open-source tools fire up supply chain attacks, 16 January 2024
- splunk, Enter the gates: an analysis of the DarkGate AutoIt loader, 17 January 2024
- The Register, Combination of cheap .cloud domains and fake Shark Tank news fuel unhealthy wellness scams, 17 January 2024
- CISCO TALOS, Exploring malicious Windows drivers (Part 1): Introduction to the kernel and drivers, 18 January 2024
- Ars Technica, Researcher uncovers one of the biggest password dumps in recent history, 18 January 2024
- Morphisec, Chae$ Chronicles: Version 4.1 Dedicated to Morphisec Researchers, 18 January 2024
- Chainalysis, 2024 crypto crime trends: illicit activity down as scamming and stolen funds fall, but ransomware and darknet markets see growth, 18 January 2024
- Google Threats Analysis Group, Russian threat group COLDRIVER expands its targeting of Western officials to include the use of malware, 18 January 2024
- Security brief, 71% of Australian small businesses view cyber-attacks as major risk, 19 January 2024
- Mandiant, Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021, 19 January 2024
- Verdict, The rise of cyber extortion and 'Hacktivism', 22 January 2024
- Cyberint, Blink-and-Update: All About Rhadamanthys Stealer, 22 January 2024
- The Hacker News, FTC bans InMarket for selling precise user location without consent, 22 January 2024
- ASEC, Various LSASS credentials dumping methods detected by EDR, 22 January 2024
- LAWFARE, New Russian Disinformation Campaigns Prove the Past Is Prequel, 22 January 2024, 22 January 2024
- Reversing Labs, GitGot: GitHub leveraged by cybercriminals to store stolen data, 23 January 2024
- Trend micro, Kasseika Ransomware Deploys BYOVD Attacks, Abuses PsExec and Exploits Martini Driver, 23 January 2024
- AFP, Un nouveau rapport de KnowBe4 montre une augmentation importante des attaques dans le secteur public en 2023, 23 January 2024
- Artic wolf, CherryLoader: A new go-based loader discovered in recent intrusions, 23 January 2024
- The conversation, The top risks from technology that we'll be facing by the year 2040, 23 January 2024
- UK National Cyber Security Centre, Cyber Essentials: are there any alternative standards?, 23 January 2024
- National Cyber Security Centre, The near-term impact of AI on the cyber threat, 24 January 2024
- Barracuda, Barracuda's new Cybernomics 101 report uncovers the financial forces driving cyberattacks, 24 January 2024

- Researcher Blog - ITOCHU Cyber & Intelligence Inc., The endless struggle against APT10: Insights from LODEINFO v0.6.6 - v0.7.3 analysis, 24 January 2024
- We live security, NSPX30: A sophisticated AitM-enabled implant evolving since 2005, 24 January 2024
- CISCO TALOS, Significant increase in ransomware activity found in Talos IR engagements, while education remains one of the most-targeted sectors, 24 January 2024
- FORTRA, WaterISAC: 15 security fundamentals you need to know, 24 January 2024
- Australian Signals Directorate, Engaging with Artificial Intelligence (AI), 24 January 2024
- 404 Media, Inside a global phone spy tool monitoring billions, 24 January 2024
- Bitdefender, Investigating worldwide SMS scams, and tens of millions of dollars in fraud, 25 January 2024
- Microsoft, Midnight Blizzard: Guidance for responders on nation-state attack, 25 January 2024
- The Hacker News, SystemBC malware's C2 server analysis exposes payload delivery tricks, 25 January 2024
- ET CIO South Asia, A world of cyber-led geopolitical and technological transitions: WEF report's breakdown, 25 January 2024
- Bleeping Computer, 23andMe data breach: Hackers stole raw genotype data, health reports, 25 January 2024
- KrebsonSecurity, Using Google search to find software can be risky, 25 January 2024
- WIRED, A last-ditch plan to save the crypto industry, 26 January 2024
- Trustwave, Spoofing 802.11 Wireless Beacon Management Frames with Manipulated Power Values Resulting in Denial of Service for Wireless Clients, 26 January 2024
- Bleeping Computer, Exploits released for critical Jenkins RCE flaw, patch now, 28 January 2024
- Security Week, Vulnerabilities in WatchGuard, Panda security products lead to code execution, 29 January 2024
- Trustwave, Trusted domain, hidden danger: Deceptive URL redirections in email phishing attacks, 29 January 2024
- IT Social, Le phishing reste toujours une sérieuse menace pour les entreprises, 29 January 2024
- The Cyber Express, The Intricacies of Atomic Stealer (AMOS) and the Emergence of Xehook Stealer on Dark Web, 29 January 2024
- Global Security Mag, Panorama de la cybercriminalité du CLUSIF : Florilège d'attaques en 2023, January 2024
- PWC, El uso de IA generativa para ciberdefensa, en la hoja de ruta de las organizaciones, January 2024
- UNODC, Casinos, Money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat, January 2024
- eucrim, Electronic Evidence, January 2024
- Network Contagion Research Institute, A Digital Pandemic: Uncovering the Role of 'Yahoo Boys' in the Surge of Social Media-Enabled Financial Sextortion Targeting Minors, January 2024

Upcoming events

- 2 February 2024, C-PROC/TUNISIA, (in-person), Briefing session on the Tunisian accession to the Budapest Convention to local embassies, Council of Europe Office in Tunis, CyberSouth+
- 2 February 2024, C-PROC/TUNISIA, (in-person), Briefing session on the Tunisian accession to the Budapest Convention at the monthly security meeting, The Dutch Embassy in Tunisia, CyberSouth+
- 5-9 February 2024, C-PROC/SENEGAL, E-evidence training first responders course (national pilot course), Dakar, GLACY+
- 5 February 2024, C-PROC/MOROCCO (in-person), Meeting with Ms. Rima Lablaili, Director of Co-operation and Communication, Ministry of Justice of Morocco, Rabat, CyberSouth+
- 6 February 2024, C-PROC/MOROCCO (in-person), Meeting with the Council of Europe Office in Rabat to discuss synergies and joint activities for 2024, Rabat, CyberSouth+
- 8 February 2024, C-PROC/Slovakia, (in person), Innocent Toolkit Launch Workshop, Bratislava, Slovakia, T-CY
- 8-9 February 2024, C-PROC/MOROCCO, (in-person), Contribution to the International Conference 'The Digital Transformation: a vector of an efficient and inclusive justice', Tangiers, CyberSouth+
- 13 February 2024, C-PROC, (online), Co-ordination meeting with MOMENTUM Project (INTERPOL) to discuss further collaboration and synergies in the MENA region, CyberSouth+
- January 2024, C-PROC, (online), further developments of the Octopus platform, Octopus
- January 2024, C-PROC, (online), further developments of the CYBOX platform, Octopus
- January 2024, C-PROC, (online), maintaining cyberviolence resource, 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