Cybercrime Digest

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

01 – 15 May 2024

Source: Hackernoon

Date: 14 May 2024

U.S. Leads Efforts for Rights-Respecting Global Cybercrime Treaty, Ensures Inclusive Negotiations

"While supporting accession to the Budapest Convention, the United States and its partners are also actively working to ensure that negotiations in the UN Ad Hoc Committee to elaborate a convention against cybercrime reach a positive outcome: a rights-respecting cybercrime treaty that would enable all UN member states to cooperate better in the fight against cybercrime. The United States and its partners will continue to oppose overly broad definitions of cybercrime that could be used to stifle freedom of expression, infringe on privacy, and or endanger individuals and communities." READ MORE

Source: Le Figaro

Date: 12 May 2024

Tunisie : interpellation musclée d'une avocate, un direct de France 24 interrompu

"Selon des médias, Sonia Dahmani fait l'objet d'une enquête notamment pour diffusion de « fausses informations dans le but de porter atteinte à la sûreté publique » et « incitation à un discours de la haine », en vertu du décret-loi 54. Ce décret, promulgué en septembre 2022 par le président Kais Saied, punit de jusqu'à cinq ans de prison quiconque utilise les réseaux d'information et de communication pour « rédiger, produire, diffuser (ou) répandre de fausses nouvelles […]»." READ MORE

Source: Business News Tunisia

Date: 15 May 2024

Mohamed Ali : quarante élus ont déposé une proposition de retrait de l'article 24 du décret 54

"Le député et rapporteur de la commission parlementaire des droits et des libertés, Mohamd Ali a affirmé qu'une quarantaine d'élus ont déposé une proposition de loi portant révision du décret 54. Il a assuré que le texte proposait le retrait de l'article 24 et non l'annulation de l'intégralité du décret. S'exprimant le 15 mai 2024 durant « Expresso » de Wassim Ben Larbi sur Express Fm, Mohamed Ali a indiqué que l'Assemblée des représentants du peuple (ARP) avait pour but de faire évoluer la législation en vigueur en engageant des débats et des procédures de révision des textes juridiques." READ MORE

Source: Business News Tunisia

Date: 16 May 2024

Yassine Mami : le décret 54 est caduc et doit être révisé

"« Je considère que le décret 54, notamment son article 24, est caduc… Il a été promulgué afin de mettre fin au chaos sur les réseaux sociaux et contre les actes de diffamations… Mais, il faut différencier la liberté d'expression et de penser de la diffusion de fausses informations », a-t-il déclaré. […] Des réserves ont été émises à ce sujet par le Conseil de l'Europe. Yassine Mami a affirmé que les magistrats ne faisaient qu'appliquer la loi. Il a indiqué que c'était à l'ARP de revoir la législation en vigueur." READ MORE

Source: Council of Europe

Date: 07 May 2024

Hate crimes must be unmasked, recorded and investigated, and victims supported

"Council of Europe member States should take all necessary measures and dedicate sufficient resources to prevent and combat hate crime and support its victims, in cooperation with civil society and other stakeholders. Effective, proportionate and dissuasive provisions to prevent and combat hate crime should be included in criminal law, and priority should be given to unmasking, acknowledging and recording the hate element of the crime." READ MORE

Source: National Crime Agency

Date: 07 May 2024

LockBit leader unmasked and sanctioned

"Khoroshev, AKA LockBitSupp, who thrived on anonymity and offered a $10 million reward to anyone who could reveal his identity, will now be subject to a series of asset freezes and travel bans. […] LockBit provided ransomware-as-a-service (RaaS) to a global network of hackers or 'affiliates', supplying them with the tools and infrastructure to carry out attacks […] The true impact of LockBit's criminality was previously unknown, but data obtained from their systems showed that between June 2022 and February 2024, more than 7,000 attacks were built using their services. The top five countries hit were the US, UK, France, Germany and China." READ MORE

RELATED ARTICLE: Europol, New series of measures issued against the administrator of LockBit, 07 May 2024

Source: Europol

Date: 03 May 2024

New network to target migrant smugglers in the digital domain

"The criminal market for migrant smuggling activities has continued to grow, alongside existing and new crises worldwide. At the same time, it has become apparent that while offering 'safe trips' online, migrant smugglers are ruthless in their lack of regard for the lives and safety of migrants. […] Migrant smugglers have quickly adjusted their modus operandi to profit from the opportunities offered by digital technologies to advertise and organise their illegal services and operations." READ MORE

Source: War on the Rocks

Date: 14 May 2024

File not Found: Russia is Hacking Evidence of its War Crimes

"Russia's breach of the digital depositories of war crime evidence highlights two new, troubling realities of 21st-century wars. First, it is widely recognized that perpetrators are using cyberspace and social media to organize, fund, execute, and celebrate their atrocities. Indeed, Russia has consistently deployed cyber attacks as part of its unjust war against Ukraine. Some claim that such operations have had little effect and are even backfiring. […] The hackers — once in the system — could plant false (AI-generated) images, videos, and audios that cast doubt on whether war crimes were committed by Russian combatants. […] Digital evidence pertinent to atrocities and violations of international humanitarian law, by any party to an armed conflict, is strictly off limits. This is especially the case given states' duties under customary international law to investigate and prosecute violations of the laws of war, crimes against humanity, and genocide." READ MORE

Source: Eurojust

Date: 08 May 2024

Take down of Austrian-based fraud scheme offering new type of crypto coin

"National authorities in Austria, Cyprus and the Czech Republic have taken decisive action against an online scam pretending to sell rights or tokens to an alleged new crypto currency. In a coordinated operation, supported by Eurojust and Europol, the six main suspects were arrested and six places were searched. In total, EUR 750.000 in assets, a property worth EUR 1.4 million and two cars were frozen/seized. […] In February 2018, the perpetrators closed all their social media accounts and took the fake company's homepage offline. This so-called exit scam made it clear to investors that they had been conned. They lost around EUR 6 million. Not all victims of the fraud have been identified at this stage." READ MORE

Source: Newsendip

Date: 06 May 2024

EU's proposed mechanism to combat child pornography with AI and experts' concerns about mass surveillance risks

"To combat and detect child pornography content, the European Union wants to be more active by using artificial intelligence systems, which makes a group of cyber security experts warn of mass surveillance risks. […] All digital platforms likely to be used for malicious purposes […] should use this technology to detect and report traces of child pornography material on their systems and in users' private chats. The EU justifies this measure by explaining that proactive detection of child sexual abuse is essential to prevent its spread, as public reporting will never be sufficient. In fact, almost 96% of content removed by YouTube is reported by automated detection technologies, and in most cases, this happens before the video reaches 10 views." READ MORE

RELATED ARTICLE:

Deseret News, AI child pornography is already here and it's devastating, 01 May 2024

Source: Council of Europe

Date: 13-14 May 2024

CyberSouth+ Contribution to the Multidisciplinary Conference on cybercrime and artificial intelligence challenges

"Moroccan Centre for Polytechnic Research and Innovation (CMRPI), together with the National School of Applied Sciences, Ibn Tofail University – Kénitra (ENSAK) and the Council of Europe organised a conference on the challenges posed by the artificial intelligence in the context of cybercrime. This symposium brought together stakeholders and specialists from different backgrounds, government, businesses, organisations in the field, to discuss on how to develop a framework for the ethical, responsible and transparent use of artificial intelligence, in order to deal with the risks associated with cybercrime. […] Morocco decided to use the HELP course on cybercrime, developed by the Council of Europe, to provide as many legal professionals as possible with basic education on cybercrime and electronic evidence." READ MORE

Source: The Guardian

Date: 08 May 2024

Chinese network behind one of world's 'largest online scams'

"More than 800,000 people in Europe and the US appear to have been duped into sharing card details and other sensitive personal data with a vast network of fake online designer shops apparently operated from China. An international investigation by the Guardian, Die Zeit and Le Monde gives a rare inside look at the mechanics of what the UK's Chartered Trading Standards Institute has described as one of the largest scams of its kind, with 76,000 fake websites created. […] Published in multiple languages from English to German, French, Spanish, Swedish and Italian, the websites appear to have been set up to lure shoppers into parting with money and sensitive personal data. […] The network used expired domains to host its fake shops, which experts say can help to avoid detection by websites or brand owners." READ MORE

Source: The Institute for Human Rights and Business

Date: 09 May 2024

Regulating AI is messy – can the UNGPs assist lawmakers?

"The newly adopted AI Act from the European Union (EU) is considered the world's first comprehensive legal framework for developing and deploying AI and also the strictest. The Act outlines a risk-based approach to what kind of AI is allowed to be developed and used in four risk categories: Unacceptable, High, Limited, and Minimal, and prescribes guidelines for each. […] While most States have not yet addressed national AI legislation, there are several approaches emerging which are useful to highlight: Risk based approach legislation:" READ MORE

Source: FBI San Francisco

Date: 08 May 2024

FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence

"AI provides augmented and enhanced capabilities to schemes that attackers already use and increases cyber-attack speed, scale, and automation. Cybercriminals are leveraging publicly available and custom-made AI tools to orchestrate highly targeted phishing campaigns, exploiting the trust of individuals and organizations alike. […] In addition to traditional phishing tactics, malicious actors increasingly employ AI-powered voice and video cloning techniques to impersonate trusted individuals, such as family members, co-workers, or business partners." READ MORE

Source: AP News

Date: 11 May 2024

A cyberattack forces a big US health system to divert ambulances and take records offline

"A cyberattack on the Ascension health system operating in 19 states across the U.S. forced some of its 140 hospitals to divert ambulances, caused patients to postpone medical tests and blocked online access to patient records. […] Cybersecurity experts say ransomware attacks have increased substantially in recent years, especially in the health care sector. Increasingly, ransomware gangs steal data before activating data-scrambling malware that paralyzes networks. The threat of making stolen data public is used to extort payments. That data can also be sold online." READ MORE

Source: The Royal Gazette

Date: 04 May 2024

Bermuda: Lessons learnt included in cybersecurity legislation

"Legislation was tabled in the House of Assembly to beef up cybersecurity in the wake of a crippling cyberattack on the Government last year. Michael Weeks, the Minister of National Security, tabled the Cybersecurity Act 2024 and the Computer Misuse Act 2024, which he said were « two important pieces of legislation aimed at strengthening our cyber posture in Bermuda ». A series of measures is expected to strengthen cybercrime laws and provide police and prosecutors « with the legislative tools needed to effectively investigate and prosecute cybercrimes »." READ MORE

Source: El País

Date: 14 May 2024

Las caras de la violencia en línea contra mujeres políticas

"Dos estudios muestran cómo opera la violencia digital contra mujeres que tienen voz pública o son lideresas. El objetivo es debilitar el debate público. Este será uno de los temas del foro Mujeres al poder que realiza EL PAÍS y Luminate. […] «La violencia en línea traspasa la virtualidad; tiene consecuencias concretas y visibles en las personas que la padecen; y con frecuencia, continúa literalmente por fuera de las plataformas digitales », dice el estudio. « Es un error y una minimización del problema hablar de violencia online como algo ajeno, separado, distanciado de la violencia estructural por razones de género »." READ MORE

Source: BN Americas

Date: 09 May 2024

Uruguay: Inició el proceso de cocreación de la Estrategia Nacional de Ciberseguridad

"La cocreación de esta Estrategia es liderada y coordinada por Agesic, con el asesoramiento del Consejo Asesor Honorario de Seguridad de la Información (Cahsi) y el Comité de Gestión de la Estrategia Nacional de Ciberseguridad (Cgenc). Cuenta con el apoyo del Banco Interamericano de Desarrollo (BID), el Centro de Competencia Cibernética para América Latina y el Caribe (LAC4) y la Organización de los Estados Americanos (OEA). La implementación de la Estrategia manifiesta el compromiso de Uruguay por hacer frente a las amenazas en constante evolución en el ámbito de la ciberseguridad, asegurando la resiliencia del país ante estos desafíos." READ MORE

Source: Forbes Chile

Date: 15 May 2024

Costo de secuestros de datos se incrementó un 500% en el último año ¿Cuánto cuesta un rescate promedio?

"La tasa de ciberataques para secuestro de datos ha disminuido ligeramente, pero los costos de recuperación alcanzan hasta 2.73 millones de dólares. El pago promedio de los rescates de datos tras ciberataques a empresas ha aumentado un 500% en el último año. Las organizaciones que pagaron rescates indicaron que el pago promedio fue de 2 millones de dólares, frente a los 400.000 dólares de 2023. Sin embargo, los rescates son solo una parte de los costos. […] Por segundo año consecutivo, las vulnerabilidades explotables fueron la causa más comúnmente detectada de los ataques, afectando al 32% de las organizaciones." READ MORE

Source: Noticias Día a Día

Date: 14 May 2024

El Peligro Oculto del Fútbol Online: Millones de Colombianos en la Mira de Ciberdelincuentes

"Casi el 50% de los usuarios de internet en Colombia están expuestos a los múltiples ataques informáticos de los hackers cuando ingresan a los sitios webs pirata para mirar transmisiones clandestinas de "fútbol libre" o "fútbol gratis". En más de 4 millones de hogares acceden a esos sitios clandestinos que promocionan la transmisión gratuita de partidos. Los sistemas piratas ingresan a los celulares, tablets y computadoras de los usuarios y les roban datos bancarios y de tarjetas de crédito, además de sus datos y archivos personales." READ MORE

Source: El Universal

Date: 15 May 2024

Hackean base de datos global de banco Santander, ¿afecta a México?

"El banco Santander informó que sufrió un "acceso no autorizado" a una base de datos alojada en un proveedor, pero afirmó que las operaciones y los sistemas no resultaron afectados y los clientes pueden seguir operando con seguridad. Sin embargo, la institución financiera reconoció que durante el hackeo los ciberdelincuentes tuvieron acceso a información de usuarios de Chile, España y Uruguay; así como de algunos empleados y extrabajadores. En el resto de los mercados y negocios, aseguró que no hay datos de clientes afectados, incluido México. Santander señaló que en la base de datos afectada no hay información transaccional ni credenciales de acceso o contraseñas de banca por internet que permitan operar con el banco." READ MORE

Source: Security Leaders

Date: 08 May 2024

72% das empresas brasileiras de commodities sofreram algum ataque em 2023

"A indústria de commodities, sejam agrícolas, animais, minerais, energéticos ou ambientais, constitui a base da economia nacional e global porque fornece as matérias-primas necessárias para a produção de diversos bens e serviços. No Brasil, especificamente, para se ter ideia de sua importância, representou cerca de 20% do PIB em 2023 e isto só é possível porque o agronegócio nacional é um dos grandes investidores em tecnologia e tem passado por uma forte transformação digital nos últimos anos." READ MORE

Source: Crypto ID

Date: 15 May 2024

Ataques de DDoS: como identificá-los e o que fazer se for vítima

"Atualmente, os ataques DDoS podem ser realizados isoladamente, mas frequentemente são utilizados em conjunto com outros tipos de ataques, como forma de tornar mais persuasiva a exigência de pagamento de um ransomware, causando danos significativos aos serviços da empresa-alvo e impactando diretamente na percepção dos clientes que tentam usar esses serviços. [...] Detectar esse tipo de ataque não é uma tarefa simples quando o ambiente não é monitorado por soluções pré-configuradas. Geralmente, os ataques são percebidos quando alguém tenta utilizar o serviço e percebe sua lentidão ou indisponibilidade." READ MORE

Source: We Live Security

Date: 13 May 2024

Ataque a sistemas Windows para minerar criptomoedas e exfiltrar informações via Telegram

"O Laboratório de Pesquisa da ESET América Latina analisou um código malicioso que afeta os sistemas operacionais Windows, detectado por nossas soluções de segurança como Python/PSW.Agent.BHH. A equipe de pesquisa da ESET observou que existe a tentativa por parte de cibercriminosos de comprometer os sistemas que utilizam versões antigas do sistema operacional Windows Server, como o Windows Server 2008 ou Windows Server 2012, versões que já não recebem atualizações de segurança da Microsoft, o que representa um risco potencial para seus usuários." READ MORE

Source: Council of Europe

Date: 13-16 May 2024

CyberSouth+ Training of Trainers on Cybercrime and E-evidence for Magistrates in Algeria

"The CyberSouth+ project, a joint action of the European Union and of the Council of Europe, organised a training of trainers course for magistrates, in Kolea, Algeria, during 13-16 May 2024. The Algerian High School for Magistrates has already adopted basic and advanced cybercrime training modules and a national pool of experts was established with the support of the previous CyberSouth project. Through this activity, the number of Algerian magistrates that can deliver training modules on cybercrime and electronic evidence to their peers has been significantly increased." READ MORE

Source: Morocco World News

Date: 01 May 2024

Cyber Mafias Hold Moroccans Captives on Thailand-Myanmar Border

"According to converging media reports, the individuals have been coerced into laboring for cybercriminal syndicates engaged in criminal activities such as fraudulent cryptocurrency transactions and e-commerce scams. According to a report from news website Euro Dayfr, the Moroccans have been subjected to abduction, torture, and exploitation at the hands of armed groups operating in the lawless border region in Southeast Asia. […] A report from the United Nations revealed that over 200,000 individuals are currently being forcibly detained, and forced to engage in romance-investment schemes and cryptocurrency fraud." READ MORE

Source: Channels TV

Date: 03 May 2024

Nigeria: NSA Orders Enforcement Of Cybercrimes Law

"On July 6, 2022, Nigeria joined 66 other countries that had signed and ratified the Budapest Convention on Cybercrime to enhance international cooperation, provide a common platform and procedural tools for efficient, and safe cyberspace under Section 41(2)(a) of the Cybercrime Act 2015, requiring conformity of Nigerian cybercrime and cybersecurity laws and policies with regional and international standards. The National Security Adviser, Nuhu Ribadu, has called for the full implementation of the Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024, including the operationalisation of the National Cybersecurity Fund by all regulators and businesses specified in the second schedule of the Act." READ MORE

Source: Nairametrics

Date: 09 May 2024

US to deploy cybercrime advisor in Nigeria to combat fraud scams, sextortion

"The United States has announced that it plans to deploy a cybercrime advisor in Nigeria. The advisor is poised to facilitate cooperation between the two nations, offering essential training, equipment, and technical assistance to bolster Nigeria's capacity to address cyber threats, including fraud scams and sextortion. […] The United States, recognizing Nigeria's progress, also commended the country for acceding to the Budapest Convention on Cybercrime in 2023 and its active participation in various cybercrime forums. […] In Nigeria, the Cybercrimes (Prohibition, Prevention etc.) Act 2015 was introduced as the legal framework for the codification of criminal activities in cyberspace. There are ongoing plans to amend this Act." READ MORE

Source: Cipesa

Date: 03 May 2024

Does Kenya's Digital Health Act Mark A New Era for Data Governance and Regulation?

"In October 2023, Kenya enacted the Digital Health Act which seeks to promote the safe, efficient and effective use of technology for healthcare and to enhance privacy, confidentiality and security of health data. It also provides for the safe transfer of personal, identifiable health data and medical records to and from health facilities within and outside Kenya, and the development of standards for provision of m-Health, telemedicine, and e-learning." READ MORE

Source: Cameroon Concord

Date: 15 May 2024

Cybercrime: Cameroonian Arrested in Zambia

"A Cameroonian national is among 77 individuals arrested in Lusaka, Zambia, as part of a large-scale anti-fraud operation conducted by Zambian authorities. […] According to reports, Golden Top Services, the Chinese company at the center of the fraud, employed Zambian nationals aged between 20 and 25. These individuals were allegedly involved in fraudulent activities on the internet, engaging in deceptive conversations with mobile users on platforms such as WhatsApp, Telegram, and discussion forums, using scripted dialogues. During the raid, authorities seized 11 SIM boxes, 13,000 SIM cards, two firearms, 78 cartridges, and two vehicles." READ MORE

Source: L'Orient - Le Jour

Date: 07 May 2024

Liban : Réseau de pédophiles sur TikTok : deux nouveaux suspects arrêtés

"Deux nouveaux suspects - à l'identité non divulguée - ont été arrêtés durant le week-end écoulé, portant jusqu'à présent à huit, le nombre de personnes interpellées par les autorités dans le cadre du dossier d'agressions sexuelles sur mineurs impliquant des influenceurs sur le réseau social TikTok. L'affaire avait éclaté au grand jour mercredi dernier, lorsque les médias locaux en avaient relaté certains détails, suite à la décision des parents de huit jeunes, il y a plus d'un mois, de porter plainte devant le parquet général contre l'un des suspects pour les sévices subis par leurs enfants." READ MORE

Source: Parliament of the Republic of Fiji

Date: 07 May 2024

Fiji is Vulnerable to Cyber-attacks and Harmful Online Activities – Speaker of the Fijian Parliament

"Fiji, like many other developing countries is vulnerable to cyber-attacks and harmful online activities such as cyber bullying, harassment, stalking and use of the internet for criminal ends. We all agree that cybercrime is one of the biggest threats to security, public safety and economic development. These were the comments by the Speaker of Parliament the Hon. Ratu Naiqama Lalabalavu whilst opening the two-days Regional Pacific Islands Parliamentary Workshop on Cybercrime. « There is no doubt that a significant part of our lives from financial services, health to education; and even Parliamentarian's lives are increasingly dependent on online or electronic modes of communications and transactions.».” READ MORE

Source: The Odessa Journal

Date: 01 May 2024

Hackers from Anonymous threaten to release data of Georgian government officials

"The international hacker and activist group, Anonymous, has expressed support for protesters in Georgia against the « foreign agents » law and threatened the government of the « Georgian Dream » with cyberattacks and data disclosure. […] Anonymous refers to themselves as « hacktivists » and claim to act according to a certain ideology and « punish » governments, corporations, and organizations with which they disagree. Anonymous is attributed with dozens of cyberattacks on governments of many countries worldwide. They have blocked websites of government agencies and corporations in the USA, Israel, Tunisia, Uganda, and other countries, as well as PayPal, MasterCard, Visa, and Sony.” READ MORE

Source: U.S. Department of Justice

Date: 01 May 2024

Sodinokibi/REvil Affiliate Sentenced for Role in $700M Ransomware Scheme

"A Ukrainian national was sentenced today to 13 years and seven months in prison and ordered to pay over $16 million in restitution for his role in conducting over 2,500 ransomware attacks and demanding over $700 million in ransom payments. […]” READ MORE

Source: BBC

Date: 14 May 2024

Christie's £670m art auctions hit by cyber attack

"The outage began last week, but the historic auction house was still able to hold a charity auction for watches on Friday in Geneva, which was itself postponed from its original 2023 date. The Only Watch auction raised 28m Swiss Francs (£26.4m) to accelerate research into Duchenne muscular dystrophy. Christie's New York auctions will begin on Tuesday with the sale of works owned by art collector Rosa de la Cruz, to be followed by art collections spanning the 20th and 21st centuries. The 20th century art collection, itself valued at $500m, includes art by Pablo Picasso, Georgia O'Keefe and Andy Warhol.” READ MORE

Source: Security Affairs

Date: 12 May 2024

Pro-Russia Hackers Targeted Kosovo's Government Websites

"Pro-Russia hackers targeted Kosovo government websites, including the websites of the president and prime minister, with DDoS attacks. The attacks are a retaliation for Kosovo's support of Ukraine with military equipment. Defense Minister Ejup Maqedonci claimed that Russian hackers launched a cyberattack against Kosovo in retaliation for his statement supporting Ukraine at the Defence 24 conference in Poland. The attacks caused temporary disruption, however, the government's Information Society Agency restored the websites. The attack is part of a hybrid war aimed at destabilizing Kosovo's security, stability, and welfare institutions, Prime Minister Albin Kurti told local media." READ MORE

Source: AlJazeera

Date: 07 May 2024

UK Defence Ministry targeted in cyberattack: Minister

"Britain's Ministry of Defence has been the target of a large-scale cyberattack, a government minister confirmed to British media. […] It targeted a third-party payroll system used by the Defence Ministry and included the names and bank details of current and former service personnel of the armed forces, Sky News and the BBC reported. […] « Targeting the names of the payroll system and service personnel's bank details, this does point to China because it can be as part of a plan, a strategy to see who might be coerced, » […]." READ MORE

Source: The America Times

Date: 08 May 2024

Joint Statement on the Inaugural U.S.-Sweden Cyber and Digital Dialogue

"The United States and Sweden held their inaugural bilateral Cyber and Digital Dialogue on May 2, 2024, in Washington, DC. The United States and Sweden affirmed their ongoing partnership on cyberspace and digital policy issues. Both sides reiterated their commitment to promote an open, free, global, interoperable, secure, and reliable Internet and stable cyberspace, and to protect and respect human rights online. […] Both sides discussed further coordination to advocate for third countries to enact legislation in line with the provisions of the Convention on Cybercrime of the Council of Europe (Budapest Convention) and engage in accession to the treaty." READ MORE

Latest reports

- TrendMicro, Router Roulette: Cybercriminals and Nation-States Sharing Compromised Networks, 01 May 2024
- Sol Cyber, The quantum apocalypse: What is post-quantum cryptography, and why do we need it? (Part 1 of 2), 01 May 2024
- InfoSecurity Magazine, DBIR: Vulnerability Exploits Triple as Initial Access Point for Data Breaches, 01 May 2024
- World Economic Forum, Cybersecurity lessons from Latin America's battle against ransomware threats, 02 May 2024
- VoxUkraine, Gender Inequality in the "Black Mirror": How to Overcome Violence in the Digital Dimension?, 02 May 2024
- Wire19, Global ransomware attacks grew by 53% in 2023: Almond Threat Landscape 2023-2024, 03 May 2024
- Save the Children, Children in Pacific Island Countries Face Increasing Levels of Violence, 06 May 2024
- The Regulatory Review, Is AI-Facilitated Gender-Based Violence the Next Pandemic?, 06 May 2024
- FindBiometrics, Biometric Data Breach Impacts 80% of El Salvador Population: Report, 06 May 2024
- CyberScoop, Stealing cookies: Researchers describe how to bypass modern authentication, 06 May 2024
- PDucklin, Listen now: The Closed Loop Conundrum and self-fulfilling failures, 07 May 2024
- SecureList, Exploits and Vulnerabilities in Q1 2024, 07 May 2024
- All Africa, Ethiopia: Research Exposes Normalization of Gender-Based Online Violence Against Women in Ethiopia, 09 May 2024
- Cigi Online, Bridging Kenya's Digital Divide: Context, Barriers and Strategies, 09 May 2024
- CCIT, Ciberseguridad en el sistema financiero colombiano: entre la amenaza y la resiliencia, 09 May 2024
- SecureList, APT trends report Q1 2024, 09 May 2024
- ProofPoint, Cybersecurity Stop of the Month: Impersonation Attacks that Target the Supply Chain, 14 May 2024
- We Live Security, Ebury is alive but unseen: 400k Linux servers compromised for cryptocurrency theft and financial gain, 14 May 2024
- InfoSecurity Magazine, Hackers Use DNS Tunneling to Scan and Track Victims, 14 May 2024
- Malware.News, Analysis of the World-First Cybercrime Index, 15 May 2024

Upcoming events

- 13-16 May 2024, C-PROC/ALGERIA, (in person), Training of Trainers on cybercrime and electronic evidence for magistrates, CyberSouth+
- 13-17 May 2024, C-PROC/ECUADOR, (in person), Pilot delivery of the specialised module on gendered aspects of cybercrime (train the trainers), GLACY-e
- 17 May 2024, C-PROC/ECUADOR, (in person), Awareness workshop with the Parliament on the Budapest Convention, GLACY-e
- 14-16 May 2024, C-PROC/HUNGARY, Meeting of US – Eastern European Cryptocurrency working group, with US Department of Justice, Workshop on Darknet, Ransomware and the move to Monero, with US Department of Justice, CyberSEE
- 16-17 May 2024, C-PROC/POLAND, ECTEG General Assembly, CyberSEE
- 17 May 2024, C-PROC/EAP, (online), Online workshop on Second Protocol - EU requirements, CyberEast+
- 20-22 May 2024, C-PROC/THE GAMBIA, (in person), Awareness workshop with the Parliament on the Budapest Convention, GLACY-e
- 21 May 2024, T-CY, (online), Bureau meeting, T-CY
- 21-22 May 2024, T-CY/DIGITAL PARTNERSHIP/FRANCE, (in person), Digital Partnership workshop, T-CY
- 21-22 May 2024, C-PROC/CAMEROON, (online), Introductory course on Budapest Convention for the task force involved in the legislative reform on cybercrime and electronic evidence, GLACY-e
- 20-24 May 2024, C-PROC/MAURITIUS, (in person), Regional virtual assets training, GLACY-e
- 20-22 May 2024, C-PROC/COLOMBIA, (in person), Regional workshop on Second Additional Protocol for LATAM, GLACY-e
- 23 May 2024, C-PROC/COLOMBIA, (in person), High level national workshop on the cybercrime legislation and round table to agree on the road map for a legislative reform, GLACY-e
- 23 May 2024, T-CY/CYBERSOUTH/MOROCCO, (in person), Workshop on the penal code (TBC), T-CY
- 23-24 May 2024, C-PROC/BOSNIA AND HERZEGOVINA, Workshop on electronic evidence for law enforcement, judges and prosecutors, with DoJ; Workshop on seizure of cryptocurrencies and money laundering, with DoJ, CyberSEE
- 27-28 May 2024, C-PROC/TURKIYE, International Conference on International Judicial Cooperation in Criminal Matters and Cybercrime; Provide guidance on practical use of Articles 8, 9, 10 and 12 of the SAP and relevant templates for requests, CyberSEE
- 27-28 May 2024, C-PROC/MOLDOVA, (in person), Meeting on cybercrime legislation reforms / Workshop on the Second Protocol / Project country team coordination, CyberEast+
- 27-28 May 2024, C-PROC/TURKIYE, International Conference on International Judicial Cooperation and Cybercrime, CYBERKOP
- 28-29 May 2024, C-PROC/MONTENEGRO, Regional workshop on strategies and practices of law enforcement training on cybercrime and electronic evidence, with DoJ and Police Academies in the region; Domestic meeting on implementation or update of cybercrime/electronic evidence training in law enforcement training institutions of Bosnia and Herzegovina; Domestic meeting on implementation or update of cybercrime/electronic evidence training in law enforcement training institutions of Serbia; Domestic meeting on implementation or update of

cybercrime/electronic evidence training in law enforcement training institutions of Turkiye, CyberSEE

- 28-30 May 2024, C-PROC/CAMEROON, (in person), Advisory mission on legislation, GLACY-e
- 28 May 2024, C-PROC/GLOBAL, (online), Fourth webinar of the fourth practitioner-to-practitioner series (under the framework of the International Network of Judicial Trainers) - OCSEA case, GLACY-e
- 29-31 May 2024, C-PROC/FRANCE, (in person), Participation of Filipino case officers in in the INTERPOL Digital Piracy Workshop, GLACY-e
- 30-31 May 2024, C-PROC/ARMENIA, (in person), Advanced cybercrime training: Advisory mission on financial investigations, CyberEast+
- 31 May 2024, C-PROC/CAMEROON, (in person), Stakeholder workshop on the role and responsibilities of 24/7 POC, GLACY-e

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