Cybercrime Digest

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

16 – 30 April 2024

Source: Council of Europe

Date: 19 April 2024

Sierra Leone acceded to the Convention on Cybercrime

"On 19 April 2024, the Embassy of Sierra Leone in Brussels deposited the instrument of accession to the Convention on Cybercrime (ETS 185). With Sierra Leone's accession, 71 States are now Parties, two have signed it and 20 have been invited to accede to the Convention." READ MORE

Source: Council of Europe

Date: 23 April 2024

Grenada accedes to the Convention on Cybercrime

"On 22 April 2024, Grenada deposited the instrument of accession to the Convention on Cybercrime (ETS 185). With Grenada's accession, 72 States are now Parties, two have signed it and 19 have been invited to accede to the Convention. Grenada joining the Convention on Cybercrime may set an example for other countries of the Caribbean region to follow." READ MORE

Source: Europol

Date: 18 April 2024

International investigation disrupts phishing-as-a-service platform LabHost

"This week, law enforcement from 19 countries severely disrupted one of the world's largest phishing-as-a-service platform, known as LabHost. This year-long operation, coordinated at the international level by Europol, resulted in the compromise of LabHost's infrastructure. Between Sunday 14 April and Wednesday 17 April a total of 70 addresses were searched across the world, resulting in the arrest of 37 suspects." READ MORE

RELATED ARTICLES:

PCMag Uk, Investigators Disrupt Phishing Page Creator LabHost, Arrest 37 Suspects, 18 April 2024

BBC, Police bust global cyber gang accused of industrial-scale fraud, 18 April 2024

ABC Net, Five Australians among 37 arrested over global phishing scam following international investigation, 18 April 2024

Source: European Parliament

Date: 24 April 2024

New EU rules to combat money-laundering adopted

"The European Parliament has adopted a package of laws strengthening the EU's toolkit to fight money-laundering and terrorist financing. The new laws ensure that people with a legitimate interest, including journalists, media professionals, civil society organisations, competent authorities, and supervisory bodies, will have immediate, unfiltered, direct and free access to beneficial ownership information held in national registries and interconnected at EU level. In addition to current information, the registries will also include data going back at least five years." READ MORE

Source: IWF

Date: 25 April 2024

IWF declares a record year for online child sexual abuse reports at Annual Report 2023 launch

"The Internet Watch Foundation (IWF) revealed a concerning increase in the amount of online child sexual abuse material at its annual report launch held in London on Tuesday (April 23, 2024). At the event, IWF CEO Susie Hargreaves OBE said that 2023 had been an "incredibly fast-paced year" in which IWF analysts had found more child sexual imagery than any year previously – more than 275,000 URLs (webpages) had been actioned by the IWF Hotline." READ MORE

RELATED ARTICLES:

PlanetRadio UK, 800% increase in number of children being blackmailed online over nude images, 18 April 2024

IWF, Under sixes manipulated into 'disturbing' sexual abuse while playing alone online as IWF says regulation can't wait, 23 April 2024

Source: Eurojust

Date: 26 April 2024

Eurojust focuses on more attention for victims' rights in cross-border judicial cooperation

"Eurojust aims to step up its efforts to assist victims of crime. The Agency will work on ways to more effectively integrate victims' rights into every step of judicial cooperation processes by national authorities: from the identification of victims to their right to remediation. This is the main outcome of the 'Symposium on Victims' Rights in Europe' organised by Eurojust this week in cooperation with the Belgian Presidency of the Council of the European Union. […] Other key partners such as the EU Centre of Expertise for Victims of Terrorism and the European Network on Victims' Rights participated in the Eurojust symposium, which focused on specific groups, such as victims of terrorism, trafficking in human beings, economic crime and cybercrime." READ MORE

Source: Reuters

Date: 29 April 2024

EU to probe Meta over handling of Russian disinformation, FT reports

"Brussels is set to open a probe into Meta Platforms' (META.O), opens new tab Facebook and Instagram as soon as Monday over concerns the company is failing to do enough to counter disinformation from Russia and other countries, the Financial Times reported. Regulators suspect that Meta's moderation does not go far enough to stop the widespread dissemination of political advertising that risks undermining the electoral process, the European Commission is expected to say on Monday, according to the report, opens new tab, which cited two people with knowledge of the matter." READ MORE

RELATED ARTICLE:

Techopedia, EU to Investigate Meta Over Election Disinformation Handling, 29 April 2024

Source: Europol

Date: 21 April 2024

European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out

"European Police Chiefs are calling for industry and governments to take urgent action to ensure public safety across social media platforms. Privacy measures currently being rolled out, such as end-to-end encryption, will stop tech companies from seeing any offending that occurs on their platforms. It will also stop law enforcement's ability to obtain and use this evidence in investigations to prevent and prosecute the most serious crimes such as child sexual abuse, human trafficking, drug smuggling, homicides, economic crime and terrorism offences." READ MORE

Source: Dig Watch

Date: 17 April 2024

UNDP confirms ransomware attack

"The United Nations Development Programme (UNDP) confirmed that it had fallen victim to a ransomware attack targeting the UNDP's IT infrastructure in Copenhagen. According to the agency, a locally hosted server was breached, resulting in data theft. The compromised information included personally identifiable details of current and former personnel, as well as procurement data concerning certain suppliers and contractors. UNDP has taken steps to notify affected individuals and entities with current contact information, promising ongoing updates as more information surfaces." READ MORE

Source: Cronica Puebla

Date: 27 April 2024

La crisis del cibercrimen en México, amenaza para economía y seguridad

"[…]La magnitud del cibercrimen en México es alarmante. Según datos recientes, el costo económico de la ciberdelincuencia en el territorio mexicano ha experimentado un aumento vertiginoso. En 2022, se estimó en 41 mil 290 millones de dólares estadounidenses. Para 2023, esta cifra se elevó a más de 60 mil millones de dólares, y se proyecta que en 2024 alcance la asombrosa cifra de 200 mil millones de dólares. Estas cifras colocan a México entre los cinco países más atacados por hackers en todo el mundo, con consecuencias desastrosas para su economía y seguridad. ¿Por qué México se ha convertido en uno de los blancos preferidos de hackers a nivel mundial?" READ MORE

Source: Techtegia

Date: 29 April 2024

Banca en Chile se enfrenta a un escenario complejo por el aumento de fraudes

"La banca en Chile se enfrenta a un panorama complejo en materia de fraude, con un aumento exponencial de delitos como el autofraude, el phishing, smishing, vishing, malware, ransomware y páginas web fraudulentas. Las pérdidas por fraude solo en autofraude alcanzaron los USD 275 millones en 2023. Según la Comisión para el Mercado Financiero (CMF), el fraude ha generado pérdidas brutas de USD 275 millones en el último año, un 105% más que el año anterior. Esto ha impactado significativamente los resultados del sector y ha obligado a las entidades financieras a destinar importantes recursos a la prevención y la restitución de fondos a los clientes afectados." READ MORE

Source: USM Chile

Date: 18 April 2024

CHILE: Nueva ley marco de ciberseguridad

"Hace unos días tuvimos una importante noticia en Chile. La publicación en el Diario Oficial de la nueva Ley Marco de Ciberseguridad. Una ley que define la institucionalidad de esta materia en el país. Pero ¿qué capacidades instaura? Una de las más importantes es la creación de una Agencia Nacional de Ciberseguridad, ANCI. Su rol será definir, aplicar y fiscalizar la política existente y proponer evoluciones. También define los servicios esenciales, es decir, las empresas privadas o las organizaciones estatales que son vitales para el funcionamiento del país." READ MORE

Source: CNN Brasil

Date: 25 April 2024

Brasil: Megaoperação contra golpes na internet prende grupo em SP e DF e derruba 540 sites

"As polícias civis do Distrito Federal (PCDF) e de São Paulo (PCSP) deflagraram uma megaoperação em São Paulo nesta quinta-feira (25) para desarticular uma organização criminosa especializada em golpes cibernéticos. Os policiais cumprem 12 mandados de prisão, 10 de busca e apreensão, bloqueio de 50 contas bancárias dos investigados e a derrubada de 540 domínios de sites falsos. A PCDF indiciou ao todo 61 pessoas na investigação. Segundo a Polícia Civil do DF, o grupo criminoso alvo da operação desta manhã já operava há pelo menos cinco anos com o conhecido golpe do falso site de leilão de carros. Para operacionalizar o esquema, os criminosos selecionavam websites reais de famosas empresas do ramo de leilão de veículos. Então clonavam esses sites, criando outros idênticos." READ MORE

Source: Convergencia Digital

Date: 22 April 2024

Brasil: Grupo especial contra cibercrime vai turbinar atuação do MPF

"O Ministério Público Federal criou o Grupo de Atuação Especial no Combate aos Crimes Cibernéticos e aos Crimes praticados mediante o uso de Tecnologias de Informação (Gaccti). O objetivo do grupo é auxiliar os chamados procuradores naturais (membros do MPF que têm atribuição jurisdicional para atuar num determinado caso específico) nas investigações e ações criminais e cíveis de prevenção e repressão a crimes cibernéticos." READ MORE

Source: APS Senegal

Date: 25 April 2024

SENEGAL-SERVICES / Lutte contre la cybercriminalité mobile: Wave manifeste sa volonté de coopérer avec les pouvoirs publics sénégalais

"La directrice nationale de Wave Digital Finance, Coura Tine Sène, a rappelé, jeudi, à Dakar, la nécessité de renforcer le partenariat entre cette société de transfert d'argent et la direction de la police judiciaire, pour mieux lutter contre la cybercriminalité et les transactions illicites. "Ce partenariat a pour objectif une étroite collaboration avec la direction de la police judiciaire, les forces de sécurité, dont la Gendarmerie nationale, les autorités administratives indépendantes, la Cellule nationale de traitement des informations financières et la Commission de protection des données personnelles, par exemple, ainsi que les autres opérateurs", a-t-elle dit." READ MORE

Source: Benin WebTV

Date: 17 April 2024

Bénin: 24 jeunes reconnus coupables de cybercriminalité condamnés à diverses peines de prison

"La cour de répression des infractions économiques et du terrorisme a prononcé une décision concernant plusieurs affaires de cybercriminalité le mardi 16 avril 2024. Un nombre significatif de cybercriminels ont été condamnés à de longues peines d'emprisonnement pour escroquerie en ligne. Les condamnations ont été prononcées le mardi 16 avril 2024 par la Cour de répression des infractions économiques et du terrorisme (CRIET)." READ MORE

Source: E-crime Bureau

Date: 20 April 2024

Kenya's Equity Bank Hit by $2.1 Million Debit Card Fraud, 19 Suspects Arrested

"Equity Bank, Kenya's biggest bank, was the target of a debit card fraud in which the perpetrators stole $2.1 million. According to a letter sent to the Directorate of Criminal Investigation, the stolen funds were moved to over 500 bank and mobile money accounts. The bank has restricted all accounts that received those funds. A fraud detective at the DCI confirmed the incident to TechCabal and claimed 19 persons were arrested in connection with the fraud. Equity Bank declined to comment." READ MORE

Source: Council of Europe

Date: 18 April 2024

CyberSouth+ project starts its activities with 8 partners from the MENA region

"On 17 and 18 April 2024, in Lisbon the Cybercrime Programme Office launched the joint European Union - Council of Europe CyberSouth+ project with the support of the North-South Centre of the Council of Europe. Representatives from Algeria, Egypt, Jordan, Lebanon Morocco, Palestine* and Tunisia, as well as the European Commission Directorate - General for Neighbourhood and Enlargement Negotiation (DG NEAR) and project partners attended the launching event. They were provided with an overview of the results of CyberSouth project (2017-2023) as well as the CyberSouth+ objectives." READ MORE

Source: Council of Europe

Date: 24 April 2024

CyberSouth+ Meeting with Jordanian stakeholders to discuss on the cybercrime legislation and future co-operation under the new project phase

"Following the official launch of the CyberSouth+ project, the Cybercrime Programme Office of the Council of Europe had meetings with representatives of the Jordanian Ministry of Justice, Judicial Council, Judicial Institute, Financial intelligence Unit, Cybercrime Unit, Jordanian Armed Forces and Ministry of Foreign Affairs to discuss on the enhancement of the national legislation and agree on activities under the new project phase. Discussions on the Convention on Cybercrime (Budapest Convention), new data protection law and coordination between cybercrime and cybersecurity actors led to identifying further areas of co-operation." READ MORE

Source: PNA

Date: 25 April 2024

Philippines: ACG boosts cyber patrols, tracks culprits behind PBBM 'deepfake'

"The Philippine National Police - Anti Cybercrime Group (PNP-ACG) on Thursday said it has intensified cyber patrols to crack down on videos on social media that were manipulated using deepfake technology, which has also victimized President Ferdinand R. Marcos Jr. The move comes after the circulation of a video with a voice resembling that of the President, directing the Armed Forces of the Philippines to act against a particular foreign country. In a statement, PNP-ACG chief Maj. Gen. Sidney Hernia said they received a tip from a concerned citizen and found deepfake videos uploaded by "Dapat Balita" on video platform YouTube that were attributed to the President and discussed tensions in the West Philippine Sea." READ MORE

Source: Bleeping Computer

Date: 27 April 2024

Japanese police create fake support scam payment cards to warn victims

"Japanese police placed fake payment cards in convenience stores to protect the elderly targeted by tech support scams or unpaid money fraud. The cards are labeled "Virus Trojan Horse Removal Payment Card" and "Unpaid Bill Late Fee Payment Card," and were created by the Echizen Police in the Fukui prefecture in Japan as an alert mechanism. Their purpose is to warn elder victims seeking payment cards at the instructions of fraudsters." READ MORE

Source: ABS-CBN

Date: 22 April 2024

Japanese 'sugar baby' gets 9 years for scamming men

"A 25-year-old Japanese woman was given a nine-year prison sentence on Monday for defrauding three men out of a total of 155 million yen ($1 million) on a dating app and selling a manual on how to scam men out of their money. The Nagoya District Court also fined Mai Watanabe, known by the moniker "itadaki joshi Riri-chan," literally "sugar baby Riri," 8 million yen ($51,700) for the scams. Prosecutors had sought a 13-year sentence and a fine of 12 million yen." READ MORE

Source: DigWatch

Date: 29 April 2024

Australia proposes stringent online safety reforms amid legal battle with social media giant

"The Australian government is currently considering significant reforms to enhance its online safety regulations, motivated by a legal dispute involving the eSafety Commissioner and social media platform X, owned by billionaire Elon Musk. This conflict emerged over X's refusal to remove a graphic video depicting a church stabbing in Sydney. In response, Communications Minister Michelle Rowland has expedited a review of the Online Safety Act, initially set for 2025 but is now due by the end of October. The proposed changes could include extending the eSafety commissioner's powers to tackle not just explicit content like hate speech and deepfakes but also broader issues like online 'pile-ons' and male violence against women facilitated by technology." READ MORE

Source: RNZ

Date: 23 April 2024

'Not consulted': Cook Islands cryptocurrency bill 'reason for concern', justice minister says

"There is growing concern over the Cook Islands dealings on a cryptocurrency bill before parliament which allegedly could be used to hack into systems around the world. Drumcliffe, a high-value debt collector specialising in international asset seizure, hired at least two Cook Islands-based lawyers to draft the Tainted Cryptocurrency Recovery Bill 2023. Industry members say there was a lack of consultation as this bill was drafted, leaving them very concerned. Stakeholders are urging a halt to the bill's progression, citing its potential far-reaching consequences. The Cook Islands' own Crown Law says it was excluded from the drafting process." READ MORE

Source: FBCNews

Date: 26 April 2024

FIJI: Authorities sound alarm over increased scams

"Authorities are sounding the alarm over a surge in mobile money transfer scams, with fifteen individuals appearing in court since February. This concerning trend has prompted heightened vigilance and consumer awareness efforts across the country, as mobile wallets are fast becoming the preferred choice for digital financial services. Police Chief of Crime, ACP Mesake Waqa, says the Fiji Police Force's Cyber Crime Unit is working closely with the Online Safety Commission to create awareness about scams." READ MORE

Source: News 18

Date: 28 April 2024

Scamdemic: How Chinese Cyber Crime Gangs Have Made Cambodia, Myanmar Their Safe Havens

"The Telangana police this week rescued two techies who were lured by Chinese-run gangs into working a job where they were committing cyber fraud and toiling 16 hours a day while being trapped in Cambodia. These two techies are not the only Indian techies who have been lured into these jobs. Over the past years many unsuspecting Indian young IT workers have been misled and trafficked into Cambodia and Myanmar and forced to work for Chinese cyber crime gangs which operate out of these nations. […] The US state department estimates that more than 10,000 people from around the globe have been forced to work for these Chinese cyber criminals. The UN estimates are far scarier." READ MORE

Source: TVP World

Date: 26 April 2024

Ukraine claims cyber win in large-scale attack on Russia

"Ukraine's Main Directorate of Intelligence has carried out a large-scale cyber attack on Russia, paralyzing police and government servers. According to sources serving in Ukraine's special services, several servers and sites were targeted, among them those belonging to the police force, the United Russia party, as well as the ER.RU and edinros domains. Despite Russian claims to the contrary, many pages are currently down. Earlier in the day, United Russia admitted that there had been a large-scale DDoS attack on all of its electronic services." READ MORE

Source: Interfax Ukraine

Date: 29 April 2024

Ukraine takes part in cyber defence exercises Locked Shields 2024 for first time

"Ukraine for the first time took part in the cyber defence exercise Locked Shields 2024, which took place in Tallinn with the participation of more than 4,000 experts from more than 40 countries, reports the NATO office in Ukraine. […] LtC Urmet Tomp, the Exercise Director at NATO CCDCOE, said: "This exercise is a demonstration of the power of international cooperation, transcending borders and uniting a diverse community of experts from the public and private sectors and academia." READ MORE

Source: Security Affairs

Date: 29 April 2024

Cyber-Partisans Hacktivists Claim To Have Breached Belarus KGB

"The Belarusian hacktivist group Cyber-Partisans claims to have infiltrated the network of the country's main KGB security agency. The hackers had access to personnel files of over 8,600 employees. The Cyber-Partisans group published on its Telegram channel a series of documents as proof of the hack, including the list of the website's administrators, the underlying database, and server logs. The official website of the KGB of the Republic of Belarus has not been working for more than 2 months. And all because the Cyber Partisans got there in the fall of 2023 and pumped out all the available information." READ MORE

Source: Council of Europe

Date: 25 April 2024

Octopus project – CYBERKOP action: Specialised judicial training course on international cooperation on cybercrime and electronic evidence

"The specialised judicial training course on international cooperation on cybercrime and electronic evidence is delivered under the CYBERKOP Action of the Octopus Project, between 23 to 25 April 2024, in Pristina. Addressed to prosecutors, representatives of the Academy of Justice and domestic trainers, the course aims to further develop their knowledge and skills on the international legal standards, as well as, tools and channels for international cooperation in cybercrime cases and exchanging of electronic evidence offered by the Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol." READ MORE

Source: Security Affairs

Date: 29 April 2024

Estonia blames Russia for GPS interference that forces Finnair to suspend flights

"Finnish airline Finnair today suspended flights to Tartu, Estonia, due to interference with GPS signals over the Baltic Sea region that Estonian authorities blamed on Russia. The airport at Estonia's second city relies solely on a GPS signal for approach and landing. On Thursday and Friday, two Finnair flights from Helsinki to Tartu were forced to turn back because of GPS interference — also called jamming." READ MORE

Source: IWF

Date: 23 April 2024

German .de domain 'ruthlessly' targeted by criminal gangs profiting from the sale of child sexual abuse images and videos

"[…]nGermany's top-level internet domain .de has become a magnet for criminal gangs with a quarter of all commercial sites profiting from child sexual abuse exploiting the domain. Data revealed today (23 April) by the Internet Watch Foundation (IWF) reveals an unprecedented rise in the number of dedicated commercial child sexual abuse websites registered as .de sites. The IWF's annual report shows a staggering 783 new commercial websites were uncovered in 2023 on the .de domain**. In every instance the websites openly displayed images and videos of child sexual abuse on the homepage of each site." READ MORE

Source: FBI

Date: 18 April 2024

Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says

"[…] The overall threat from the Chinese Communist Party (CCP) is a hybrid one that involves crime, counterintelligence, and cybersecurity—and which the FBI is countering with resources from all three missional spheres, Wray said. The threat is partially "driven by the CCP's aspirations to wealth and power," Wray said, adding that China wants to "seize economic development in the areas most critical to tomorrow's economy," even if doing so requires theft. The Chinese government has tried to pilfer "intellectual property, technology, and research" from nearly every industry in the U.S. economy, he noted." READ MORE

RELATED ARTICLE:

DigWatch, FBI chief warns of Chinese hackers threatening US infrastructure, 19 April 2024

Source: US Department of Justice

Date: 18 April 2024

Justice Department Seizes Four Web Domains Used to Create Over 40,000 Spoofed Websites and Store the Personal Information of More Than a Million Victims

"United States Attorney Eric G. Olshan announced today the seizure of four domains used by the administrators and customers of a domain spoofing service. The domain seizures were authorized pursuant to seizure warrants issued in the Western District of Pennsylvania and were executed in coordination with the arrest of dozens of administrators and customers of the illicit service by foreign law enforcement agencies. According to court records, the United States obtained authorization to seize the domains as part of an investigation of the spoofing service operated through the Lab-host.ru domain (LabHost), which resolves to a Russian internet infrastructure company. LabHost provided online infrastructure and interactive functionality for its subscription-based services." READ MORE

Source: Privacy Commissioner of Canada

Date: 23 April 2024

OPC submission to Justice Canada consultation on implementing protocol to international Convention on Cybercrime

"The Office of the Privacy Commissioner of Canada (OPC) has provided feedback to a Department of Justice consultation on the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. In its submission, the OPC has recommended options for stronger oversight, safeguards, and transparency." READ MORE

Latest reports

- Cloudfare, DDoS threat report for 2024 Q1, 16 April 2024
- Watchtower, Palo Alto - Putting The Protecc In GlobalProtect (CVE-2024-3400), 16 April 2024
- ProofPoint, From Social Engineering to DMARC Abuse: TA427's Art of Information Gathering, 16 April 2024
- Interface Media, 3 emerging threats facing cybersecurity leaders in 2024, 16 April 2024
- Resecurity, Misinformation And Hacktivist Campaigns Target The Philippines Amidst Rising Tensions With China, 16 April 2024
- DigWatch, Digital dominance in the 2024 elections, 16 April 2024
- HackerNews, Widely-Used PuTTY SSH Client Found Vulnerable to Key Recovery Attack, 16 April 2024
- CyberCX, Middle East conflict: Cyber impacts of Iran-Israel military escalation, 16 April 2024
- Finance Online, 73 Important Cybercrime Statistics: 2024 Data Analysis & Projections, 16 April 2024
- Tripwire, Navigating AI and Cybersecurity: Insights from the World Economic Forum (WEF), 17 April 2024
- MinterEllison, Perspectives on Cyber Risk 2024, 17 April 2024
- BlackBerry, Threat Group FIN7 Targets the U.S. Automotive Industry, 17 April 2024
- Securelist, SoumniBot: the new Android banker's unique techniques, 17 April 2024
- Zscaler Blog, Malvertising campaign targeting IT teams with MadMxShell, 17 April 2024
- Mandiant, Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm, 17 April 2024
- Sophos, 'Junk gun' ransomware: Peashooters can still pack a punch, 17 April 2024
- Talos, OffiRouter virus causes Ukrainian users to upload confidential documents to VirusTotal, 17 April 2024
- IAPP, Will the EU AI Act work? Lessons learned from past legislative initiatives, future challenges, 17 April 2024
- CISA, Securing Election Infrastructure Against the Tactics of Foreign Malign Influence Operations, 17 April 2024
- Schneier on Security, Other Attempts to Take Over Open Source Projects, 18 April 2024
- Open JS Foundation, Social Engineering Takeovers of Open Source Projects, April 2024
- Securelist, DuneQuixote campaign targets Middle Eastern entities with "CR4T" malware, 18 April 2024
- Medium, Advanced Cyber Threats Impact Even the Most Prepared, 19 April 2024
- Jamie Bartlett, The police have a new approach to cybercrime, 19 April 2024
- BleepingComputer, Malware dev lures child exploiters into honeytrap to extort them, 21 April 2024
- Microsoft, Analyzing Forest Blizzard's custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials, 22 April 2024
- BrainWave, Norway 2024 cybercrime report: key insights, 23 April 2024
- Carnegie Endowment for International Peace, Exploring Law Enforcement Hacking as a Tool Against Transnational Cyber Crime, 23 April 2024

- Techspective, Key Insights from Coalition's 2024 Cyber Claims Report, 24 April 2024
- Security Week, North Korean Hackers Hijack Antivirus Updates for Malware Delivery, 24 April 2024
- CISA, Cyber Hygiene Helps Organizations Mitigate Ransomware-Related Vulnerabilities, 25 April 2024
- Flashpoint, The Israel-Iran Conflict Through an Intelligence Lens, 25 April 2024
- FinTelegram, Cybercrime Surges as U.S. Insurance Claims Increase, Reveals Coalition's 2024 Cyber Claims Report, 28 April 2024
- Times of Malta, The evolution of cybercrime in the era of Artificial Intelligence, 28 April 2024
- Marcum LLP, Cybersecurity Threats Affecting Businesses in April 2024, 29 April 2024
- CheckPoint, Threat intelligence report, 29 April 2024
- The DFIR Report, From IcedID to Dagon Locker Ransomware in 29 Days, 29 April 2024
- Infoblox, A cunning operator: Muddling Meerkat and China's Great firewall, 29 April 2024
- Cyble, Threat Actor profile: SideCopy, 29 April 2024
- Krebs on Security, FCC Fines Major U.S. Wireless Carriers for Selling Customer Location Data, 29 April 2024
- Forbes, Cybercrime And The Challenge Of Static Legislations In Nigeria, 29 April 2024
- ENISA, Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report, 30 April 2024
- IWF, Annual Report 2023, April 2024
- IST's RTF Payments Working Group, Information Sharing in the Ransomware Payment Ecosystem: Exploring the Delta Between Best Practices and Existing Mechanisms, April 2024
- INTERPOL, African Cyberthreat Assessment Report, April 2024

Upcoming events

- 6 May 2024, C-PROC/PACIFIC, *(online)*, High Level workshop for policymakers of the Pacific Islands, GLACY-e
- 8-9 May 2024, C-PROC/ECUADOR, *(online)*, Stakeholder workshop on the role and responsibilities of 24/7 POC, GLACY-e
- 8-10 May 2024, C-PROC/KIRIBATI, *(online)*, Stakeholder workshop on the role and responsibilities of 24/7 POC and central authorities, GLACY-e
- 8-10 May 2024, C-PROC, *(online)*, Contribution to the ESDC course 'The EU's Cybersecurity Strategy for the Digital Decade', CyberSouth+
- 13-15 May 2024, C-PROC/MALAWI, Consultation and consolidation workshops on the draft bill on cybercrime and electronic evidence, GLACY-e
- 13-14 May 2024, C-PROC/MOROCCO, *(in person)*, Support to the 'Conference on cybercrime and the challenges of artificial intelligence', 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
- 13-16 May 2024, C-PROC/ALGERIA, *(in person)*, Training of Trainers on cybercrime and electronic evidence for magistrates, Kolea, CyberSouth+

- 14-16 May 2024, C-PROC/ HUNGARY, *(in person)*, Meeting of US – Eastern European Cryptocurrency working group, with US Department of Justice, CyberSEE
- 15 May 2024, C-PROC/KAZAKHSTAN, *(in person)*, Coordination meeting on cybercrime legislation, criminal justice capacities and the Budapest Convention with national stakeholders, Octopus project
- 15 May 2024, C-PROC/ UNITED KINGDOM, *(in person)*, Counter Ransomware Initiative Policy Pillar Meeting, CyberSEE
- 15 May 2024, C-PROC/BELGIUM, *(in person)*, Cyber Project Community Meeting, CyberSEE

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