Cybercrime Digest

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

1 - 15 February 2024

Source: Council of Europe

Date: 07 February 2024

Grenada and Mozambique have been invited to accede to the Convention on Cybercrime

"On 7 February 2024, Grenada and Mozambique have been invited to accede to the Convention on Cybercrime (Budapest Convention). This invitation to accede is valid for five years from its adoption. This is also a result of capacity building activities supported through the various projects of the Cybercrime Programme Office of the Council of Europe (C-PROC). This invitation will permit more support by the Council of Europe under the GLACY-e and Octopus Project." READ MORE

RELATED ARTICLES:

Africa Cybersecurity Magazine, La Grenade et le Mozambique sont désormais adhérents à la Convention de Budapest sur la cybercriminalité, 8 February 2024

Source: Council of Europe

Date: 02 February 2024

Octopus project: Japan makes a voluntary contribution

"The Government of Japan has made a voluntary contribution of €120,000 to support the Council of Europe action against cybercrime. The agreement was signed on 2 February 2024 by Ambassador Hiroyuki Uchida, Permanent Observer of Japan to the Council of Europe, and Mr Bjørn Berge, Deputy Secretary General." READ MORE

Source: dig watch

Date: 10 February 2024

No consensus for the UN Cybercrime Treaty | The Concluding Session of the Ad Hoc Committee on Cybercrime 2024

"The concluding session of the Ad Hoc Committee on Cybercrime has ended, but a consensus has not been reached. The Chair of the Ad Hoc Committee and the Secretariat submitted a draft decision to the General Assembly stating that the Ad Hoc Committee on Cybercrime will hold an additional session with a date yet to be decided. The additional session will last up to 10 days, and it aims to conclude and provide the draft convention at the General Assembly at the seventy-eighth session. Responses from delegations were mixed, to mention some Russia is pushing for two rounds of informal sessions before holding the additional session. At the same time, Lichtenstein stressed that having the additional session will significantly impact financial and personal capabilities." READ MORE

RELATED ARTICLE:

VOA, Civil society warns of 'critical gaps' in UN's draft Cybercrime Treaty, 13 February 2024

Source: Eurojust

Date: 07 February 2024

One of the key leaders of EncroChat extradited to France with the support of Eurojust

"One of the main key leaders of the company behind the encrypted communication tool EncroChat has been extradited to France from the Dominican Republic with the active support of Eurojust. The person involved was arrested in the Dominican Republic in May 2022 and has been under house arrest since then. […] This dismantling was coordinated and supported by Eurojust and Europol and sent shockwaves through organised crime. Between 2020 and 2023, over 6 500 suspects were arrested and at least EUR 900 million in assets were seized, with investigations still ongoing. Eurojust supported a joint investigation team into the case from 2020." READ MORE

Source: European Council

Date: 06 February 2024

Violence against women: Council and European Parliament reach deal on EU law

"The Belgian presidency and European Parliament agreed on a first-ever EU law on violence against women and domestic violence. The new law lays down minimum rules concerning the definition of specific criminal offences and penalties to address this form of violence. It also sets out rights of victims of all forms of violence against women or domestic violence and provides for their protection." READ MORE

Source: Europol

Date: 12 February 2024

International cybercrime malware service targeting thousands of unsuspecting consumers dismantled

"An international operation has resulted in the seizure of several internet domains that were used by cybercriminals to sell malware. Through use of this malware, cybercriminals could secretly access and connect to victims' computers for malicious purposes. The operation was led by the FBI and supported by Europol and the Joint Cybercrime Action Taskforce (J-CAT). On 7 February, two suspects were arrested in Malta and Nigeria in the framework of the operation. The suspects are accused of selling the malware and supporting cybercriminals who used the malware for malicious purposes. Europol provided analytical support to the investigation which led to the operation involving Australia, Canada, Croatia, Finland, Germany, Malta, the Netherlands, Nigeria, Romania and the United States. These countries provided valuable assistance securing the servers hosting the Warzone RAT infrastructure." READ MORE

Source: Council of Europe

Date: 06 February 2024

Celebrating Safer Internet Day 2024

"Following a process that began in 2023 and is set to be completed in 2024, an abridged version of the report "The metaverse and its impact on Human Rights, Rule of Law, and Democracy" is now available for download in electronic format. The document provides an overview of the principal issues outlined in a report on "The metaverse and its impact on Human Rights, Rule of Law, and Democracy," soon to be published." READ MORE

Source: French Diplomacy

Date: 06 February 2024

Cybersecurity – Joint communiqué of the United Kingdom and France on the Lancaster House conference to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities (London, 6 & 7 February 2024)

"On February 6 and 7, 2024, the United Kingdom and France convened a conference in Lancaster House, in London, bringing together an international multistakeholder community to discuss growing concerns around the proliferation and irresponsible use of commercial cyber intrusion capabilities. Building from the discussions initiated during the 2023 Paris Peace Forum, the United Kingdom and France launched the Pall Mall Process, an international initiative supported by a broad community of representatives from governments, the private sector and civil society. In acknowledgement of the work originated from the Paris Call for Trust and Security in Cyberspace, and acting on the direction from the 2023 French-British Leaders Summit, the Pall Mall process seeks to tackle the threat posed by commercial cyber proliferation and irresponsible use of cyber intrusion tools and services." READ MORE

RELATED ARTICLE:

Ministère de L'Europe et des affaires étrangères, The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities (Lancaster House, London, 6 February 2024), 6 February 2024

Source: WHO

Date: 06 February 2024

WHO reports outline responses to cyber-attacks on health care and the rise of disinformation in public health emergencies

"While digital tools have brought new opportunities to enhance health and well-being, they have also created new health security risks, such as cyber-attacks on health care and disinformation. To provide a clearer understanding of these risks and to reduce their likelihood and severity, WHO produced two reports, in collaboration with INTERPOL, the United Nations Office on Drugs and Crime (UNODC), the UN Office of Counter-terrorism, the UN International Computing Centre (UNICC), the UN Interregional Crime and Justice Research Institute, and the CyberPeace Institute." READ MORE

Source: Carnegie Council for Ethics in International Affairs

Date: 02 February 2024

It takes a village to protect children in the Metaverse

"[…] Today, the United Nations International Children's Emergency Fund (UNICEF) is fighting against that outmoded thinking. The UN agency is urging the international community to take heed of children's safety in virtual spaces and raising awareness that abuse, actually, "can feel more 'real' in immersive virtual environments." According to a study in the journal Child and Adolescent Psychiatry and Mental Health, psychologists concluded it is important to treat online sexual abuse as "a serious form of sexual abuse even if the victim and perpetrator have not met outside the Internet."" READ MORE

Source: Ministerio Público Fiscalía de la Nación

Date: 15 February 2024

Peru: Unidad Fiscal Especializada en Ciberdelincuencia brinda asistencia técnica para enfrentar la ciberdelincuencia

"En tres años de creación, la Unidad Fiscal Especializada en Ciberdelincuencia logró que Perú ingrese como país prioritario a la GLACY+ para prevenir y perseguir el ciberdelito en alianza con entidades nacionales y extranjeras. Al cumplir tres años de funciones, la Unidad Fiscal Especializada en Ciberdelincuencia (UFEC) atendió, de manera activa, un total de 1162 solicitudes de acompañamientos técnicos de los fiscales que investigan la comisión de delitos informáticos y aquellos en los cuales la obtención de prueba digital sea determinante para el esclarecimiento de los casos." READ MORE

Source: La Nacion

Date: 13 February 2024

Lavado de dinero: la Argentina, en peligro de ser incluida en la "lista gris"

"Hace semanas que en la Argentina la atención se ha puesto pura y exclusivamente en la discusión de la ley ómnibus; sin embargo, es importante recordar que no es lo único que está tratando el Senado. Desde mediados del año pasado se está deliberando un proyecto de modificación de la ley 25.246 en prevención del lavado de activos. De no sancionarse, la Argentina podría ser incluida en la "lista gris" del Grupo de Acción Financiera Internacional (GAFI), con consecuencias financieras graves para nuestro país." READ MORE

Source: tnt&t

Date: 12 February 2024

Trinidad and Tobago: The issues arising from new cybercrime laws

"The last meeting of the OAS discussions between government level experts on cybercrime took place in December 2016. On the agenda then were the challenges of prevention, investigation and prosecution of cybercrime and the importance of effective legislation. Those priorities are still relevant, but in the larger landscape of cybercrime, everything has changed." READ MORE

Source: Barbados Today

Date: 15 February 2024

Barbados: Controversial Cybercrime Bill goes to House-Senate review committee

"The Senate on Wednesday shelved debate on the contentious Cybercrime Bill, sending the controversial legislation to a select committee of both houses of Parliament. The joint select committee, according to a resolution introduced by Leader of Government Business Senator Lisa Cummins, will be required to report on its findings in three months. The resolution was passed without further comment." READ MORE

RELATED ARTICLES:

Barbados Today, New cybercrime legislation an 'enviable standard', 7 February 2024

Nation News, AG praises Cybercrime Bill, 7 February 2024

Source: Sierraloaded

Date: 11 February 2024

Sierra Leone ratifies Budapest Convention on cybercrime, strengthening global cybersecurity collaboration

"Sierra Leone achieved a momentous milestone on February 8, 2024. The National Cyber Security Coordination Centre (NC3) proudly announced the ratification of the Budapest Convention on Cybercrime and its First Additional Protocol on Xenophobia and Racism. This pivotal decision comes on the heels of an impactful workshop with the Council of Europe in November 2023, showcasing the nation's dedication to tackling cyber threats collaboratively." READ MORE

Source: Tunisie Numerique

Date: 06 February 2024

Cybercrime: Parliament approves Tunisia's accession to Budapest Convention

"Parliament approved on Tuesday the bill on Tunisia's accession to the Budapest Convention on Cybercrime, with 115 votes for, 9 against and 12 abstentions. As a reminder, Tunisia officially submitted to the Council of Europe in October 2017 a request to join the Budapest Cybercrime Convention, considered the most relevant international agreement on cybercrime and electronic evidence." READ MORE

RELATED ARTICLE:

Africa Cybersecurity Magazine, Effort mondial de lutte contre la cybercriminalité: La Tunisie adhère à la convention de Budapest, 13 February 2024

Source: FRANCE 24

Date: 13 February 2024

Senegal bans protest over delayed vote, suspends internet access

"Three people have been killed during violent protests after President Macky Sall's decision to push back the February 25 vote plunged traditionally stable Senegal into one of its worst crises in decades. "We are deeply concerned about the tense situation in Senegal," Liz Throssell, spokeswoman for the UN's human rights office, told reporters in Geneva. "Following reports of unnecessary and disproportionate use of force against protesters and restrictions on civic space, we call on the authorities to ensure that they uphold Senegal's long-held tradition of democracy and respect for human rights," she added." READ MORE

Source: Aljazeera

Date: 13 February 2024

Nigerian star Iwobi faces cyberbullying after AFCON loss to Ivory Coast

"In the aftermath of Nigeria's defeat on Sunday at the recently concluded Africa Cup of Nations, Nigeria midfielder Alexander Iwobi archived all of the posts on his Instagram account, leaving the page blank. The action was in response to a barrage of hate speech on his social media accounts, as disappointed Nigeria supporters sought an outlet for outrage following the Super Eagles' 1-2 loss to hosts Ivory Coast in Sunday's final." READ MORE

Source: The Daily Statesman

Date: 06 February 2024

Ghana: Cybersecurity Authority calls on stakeholders to collaborate to combat online child abuse

"The Cyber Security Authority (CSA) has emphasised the need for collaborative efforts to enhance internet safety in Ghana and across Africa. In a press statement issued by its Public Affairs Unit, the CSA underscored the necessity for stakeholder engagement to educate the public on cybersecurity threats prevalent on the internet. The statement called for a collective approach involving parents, teachers, civil society organizations, the media, and the private sector to foster safe and positive utilization of digital technology, particularly among children and young people." READ MORE

Source: NATION

Date: 14 February 2024

Kenya and US partner to fight cybercrime

"The United States government has pledged support for Kenya to help it tackle security challenges such as the rise in cybercrime and misinformation on social media. According to the Commanding Officer of the Combined Joint Task Force – Horn of Africa Major General Jami Shawley, the US government through the force is opening up training for security personnel on identifying and tackling cybercrimes in the country." READ MORE

Source: BBC

Date: 09 February 2024

Sudan hit by internet blackout as civil war continues

"Sudan has been plunged into an internet blackout with many blaming the paramilitary group fighting the army in the country's 10-month civil war. The Rapid Support Forces (RSF) has denied responsibility. NetBlocks, a watchdog that monitors internet freedom, said on X, there had been a "new collapse of internet connectivity" in Sudan." READ MORE

Source: Dark Reading

Date: 02 February 2024

South African railways lost over $1M in phishing scam

"South Africa's railway agency lost some 30.6 million rand (US$1.6 million) after the transport network fell victim to a phishing scam. In its annual report, the Passenger Rail Agency of South Africa (PRASA) said that it had recovered just over half of a the total money stolen by the criminals behind the attack. The theft remains the subject of an ongoing investigation." READ MORE

Source: Coin Telegraph

Date: 07 February 2024

South Korean crypto criminals face life imprisonment

"[…] The South Korean government has issued a new update to the Virtual Asset Users Protection Act with cryptocurrency-focused regulations that aim to protect investors from market crimes. On Feb. 7, The Financial Services Commission (FSC) — South Korea's top financial regulator — announced the new law that seeks to protect the rights of crypto investors and promote transparency." READ MORE

Source: Microsoft

Date: 06 February 2024

Iran accelerates cyber ops against Israel from chaotic start

"Since Hamas attacked Israel in October 2023, Iranian government-aligned actors have launched a series of cyberattacks and influence operations (IO) intended to help the Hamas cause and weaken Israel and its political allies and business partners. Many of Iran's immediate operations after October 7 were hasty and chaotic – indicating it had little or no coordination with Hamas – but it nevertheless has achieved growing success. […] These insights are taken from the latest biannual report on Iran from the Microsoft Threat Analysis Center (MTAC) Iran surges cyber-enabled influence operations in support of Hamas." READ MORE

RELATED REPORT:

Microsoft Security, Iran surges cyber-enabled influence operations in support of Hamas, 7 February 2024

Source: The Guardian

Date: 08 February 2024

Cyber-attacks by North Korea raked in $3bn to build nuclear weapons, UN monitors suspect

"UN sanctions monitors are investigating dozens of suspected cyber-attacks by North Korea that raked in $3bn to help it further develop its nuclear weapons programme, according to excerpts of an unpublished UN report reviewed by the Reuters news agency. "The Democratic People's Republic of Korea (DPRK) continued to flout security council sanctions," a panel of independent sanctions monitors reported to a security council committee, using North Korea's formal name." READ MORE

Source: Binding Hook

Date: 13 February 2024

Emerging technologies will intensify the North Korean cyber threat

"The World Economic Forum's Global Risk Report 2024, released in January, puts cyber insecurity as the fourth most severe global risk, up from eighth in 2023. North Korea is a major contributor to rising cyber insecurity. Its hackers stole $600 million in cryptocurrency in 2023, "almost a third of all funds stolen in crypto attacks last year", according to a report by TRM Labs. North Korea emerged as a major cyber actor on the international scene in 2014 when it hacked multinational firm Sony Pictures. It was also the first time Washington openly attributed an attack to a foreign country." READ MORE

Source: The Straits Times

Date: 04 February 2024

Singapore to host and fund ASEAN emergency response team to combat regional cyber threats

"When cyber-attacks strike important services in the region, such as energy networks, hospitals or supermarkets, nations must quickly collaborate to identify and eliminate the threats. Such scenarios are the focus of an upcoming cyber emergency response team for Asean that is being formalised and will be funded and hosted by Singapore, Communications and Information Minister Josephine Teo said on Feb 2." READ MORE

Source: Japan Times

Date: 05 February 2024

Classified Japanese diplomatic info leaked after Chinese cyberattacks

"Classified Japanese diplomatic information was leaked following Chinese cyberattacks on the Foreign Ministry in 2020, a government source said Monday, exposing the nation's digital vulnerability. Japan detected the large-scale attack and release of diplomatic telegrams during a period of government under then-Prime Minister Shinzo Abe, the source said, but the nature of the leaked information is still publicly unknown." READ MORE

Source: Reuters

Date: 09 February 2024

Philippines wards off cyber attacks from China-based hackers

"Hackers operating in China attempted to break into websites and e-mail systems of the Philippine's president and government agencies, one promoting maritime security, but failed, an information and communications ministry official said on Monday. The mailboxes of the Department of Information and Communications Technology (DICT), the website of National Coast Watch, and the personal website of Philippine President Ferdinand Marcos Jr were among the targets of the unsuccessful hacking operations in January, DICT spokesperson Renato Paraiso told DWPM radio. "We are not attributing this to any state. But using the internet protocol addresses, we pinpointed it to China," Paraiso said, adding the hackers were traced to be using the services of Chinese state-owned Unicom." READ MORE

Source: The Guardian

Date: 10 February 2024

Is my home spying on me? As smart devices move in, experts fear Australians are oversharing

"Take a look around your home and chances are you have one, or at least you have considered the convenience of having one. They are the devices and appliances that can be remotely controlled – otherwise known as smart devices – which over the past decade have become core features of the modern home. But as the technologies gather, share, aggregate and analyse the data collected, that convenience has come at a cost: privacy. Experts say consumers should be aware of how much personal information they are trading, and what that information is used for." READ MORE

Source: Ministry of Foreign Affairs of Ukraine

Date: 09 February 2024

Kyiv hosted the first Kyiv International Cyber Resilience Forum 2024: "Resilience At The Cyberwar"

"On February 7-8, 2024 Kyiv hosted the first Kyiv International Cyber Resilience Forum 2024: "Resilience At The Cyberwar". Overall, this is the first time in recent years that such a large-scale cybersecurity event has been held in Ukraine. It brought together government and business representatives, the cyber community, technology companies and leading industry experts to discuss cybersecurity. The Kyiv International Cybersecurity Forum is planned to be held annually, creating the basis for the development of a platform where best practices can be shared and joint strategies and measures to counter cyber threats can be discussed." READ MORE

Source: BBC

Date: 14 February 2024

Ransomware attack hits dozens of Romanian hospitals

"Over a hundred Romanian healthcare facilities have been affected by a ransomware attack, with some doctors forced to resort to pen and paper. Children's and emergency hospitals were among those hit, with other facilities going offline as a precaution. […] The incident was under investigation by IT specialists, including cyber security experts from the National Cyber Security Directorate (DNSC), the ministry said. According to the DNSC, 25 hospitals were affected by the attack, starting with the The Pitesti Paediatric Hospital." READ MORE

RELATED ARTICLE:

Hack Read, Ransomware attack disrupts services in 18 Romanian hospitals, 12 February 2024

Source: Bloomberg Law

Date: 06 February 2024

Dutch intelligence blames Chinese State for cyber espionage

"The Dutch intelligence agency said it uncovered a Chinese-state-backed attempt to use malware to spy on a computer network that's used by the country's armed forces. "Sophisticated" Chinese malware was found on a standalone computer that was used for unclassified research and development, the Dutch Military Intelligence and Security Service said in a statement on Tuesday. The system was self-contained and the malware didn't result in damage to the defense network, the agency said." READ MORE

Source: The Record

Date: 09 February 2024

Health insurance data breach affects nearly half of France's population, privacy regulator warns

"Data on more than 33 million people in France, approximately half the population, was compromised in a cyberattack at the end of January, according to the country's privacy watchdog. The Commission Nationale Informatique et Libertés (CNIL) announced this week it had been informed by two health insurance companies, Viamedis and Almerys, about the incident." READ MORE

Source: Office of the Government Chief Information Officer

Date: 07 February 2024

Ireland: Ministers McEntee and Browne receive approval to draft legislation to allow Gardaí swift access to digital criminal evidence

"Minister for Justice Helen McEntee and Minister of State James Browne have secured Government approval for the drafting of new legislation which will permit Gardaí to swiftly access criminal evidence in digital form. Government have today approved the General Scheme of the Criminal Justice (Protection, Preservation and Access to Data on Information Systems) Bill 2024, which will allow law enforcement authorities like An Garda Síochána to request the preservation and production of data being held on IT systems controlled by internet service providers in order to investigate and tackle crime." READ MORE

Source: Diario de Mallorca

Date: 05 February 2024

La Policía analiza en Palma las novedades de la ciberdelincuencia

"La Policía Nacional de Palma celebró la pasada semana una jornada técnica para analizar las últimas novedades del fenómeno delictivo conocido como ciberdelincuencia, ya que el número de denuncias por este tipo de estafas se ha disparado. Acudieron a este encuentro, además de los investigadores policiales, jueces y fiscales. Participaron ponentes especialistas del Banco de Santander, que detallaron las últimas novedades informáticas que facilitan este tipo de estafas electrónicas. En la charla se intercambiaron experiencias y se habló de las actuaciones que se llevan a cabo para erradicar este tipo de delincuencia tan avanzada. Todos los presentes coincidieron en que se trata de un delito que ha ido evolucionando, por lo que es preciso que la Policía cuente con los conocimientos técnicos para poder erradicarlo." READ MORE

Source: Info Security Magazine

Date: 05 February 2024

Pennsylvania Courts' Website Disrupted by DoS Attack

"The Pennsylvania Courts system has been hit by a cyber-attack, taking down parts of its website. The Administrative Office of Pennsylvania Courts revealed via social media that the service had suffered a denial of service (DoS) attack. The statement noted that court web systems such as PACFile, the use of online docket sheets and the Guardianship Tracking System were impacted by the incident." READ MORE

Source: US Department of Justice

Date: 01 February 2024

Foreign National Charged for International Money Laundering Conspiracy and Role in Operation of Unlicensed Digital Currency Exchange BTC-e

"An indictment was unsealed on Tuesday charging a Belarusian and Cypriot national with money laundering conspiracy and operation of an unlicensed money services business. […] The indictment alleges BTC-e was a significant cybercrime and online money laundering entity that allowed its users to trade in bitcoin with high levels of anonymity and developed a customer base heavily reliant on criminal activity. BTC-e allegedly facilitated transactions for cybercriminals worldwide and received criminal proceeds from numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings, and allegedly was used to facilitate crimes ranging from computer hacking to fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking." READ MORE

Latest reports

- Akamai, Frog4Shell — FritzFrog botnet adds one-days to its arsenal, 1 February 2024
- GBHackers, Hackers started using python for developing new ransomware, 1 February 2024
- UNIT 42, Exploring the latest Mispadu Stealer variant, 2 February 2024
- GBHackers, New Android Malware on Google Play disguised as messaging or news apps, 2 February 2024
- Sophos News, Cryptocurrency scams metastasize into new forms, 2 February 2024
- Security Week, Cloudflare hacked by suspected state-sponsored threat actor, 2 February 2024
- APC, APC policy explainer: Cybercrime and gender, 2 February 2024
- The Cyber Express, Anonymous collective reveals new referral program for privacy shield VPN and CloudStorm DDoS services, 5 February 2024
- ASPI, Will 2024 be the year of responsible AI?, 5 February 2024
- European Council, The EU's fight against organised crime, 5 February 2024
- Recorded Future, Essentials of cyber crime investigation, 5 February 2024
- UNIT 42, Ransomware retrospective 2024: Unit 42 leak site analysis, 5 February 2024
- Google, Buying Spying: How the commercial surveillance industry works and what can be done about it, 6 February 2024
- Proofpoint, How do cybercriminals escalate privilege and move laterally?, 6 February 2024
- ThreatDown, 2024 ThreatDown State of Malware, 6 February 2024
- Ministry of Home Affairs India, Cases of Cyber Frauds, 6 February 2024
- Krebs on Security, From Cybercrime Saul Goodman to the Russian GRU, 7 February 2024
- Check Point Research, Raspberry Robin keeps riding the wave of endless 1-days, 7 February 2024
- The Hacker News, Critical boot loader vulnerability in shim impacts nearly all Linux distros, 7 February 2024
- Secure List by Kaspersky, Coyote: A multi-stage banking Trojan abusing the Squirrel installer, 8 February 2024
- CSCIS, Cyber Intelligence Report, 8 February 2024
- GBHackers on security, Critical Cisco Expressway Flaw Let Remote Execute Arbitrary Code, 8 February 2024
- Security Week, Iran Ramps Up Cyberattacks on Israel Amid Hamas Conflict: Microsoft, 8 February 2024
- Check Point Research, Maldocs - of Word and Excel: Vigor of the ages, 8 February 2024
- Lares, I Know What Your Password Was Last Summer…, 8 February 2024
- Cisco Talos, New Zardoor backdoor used in long-term cyber espionage operation targeting an Islamic organization, 8 February 2024
- Hack Read, Hackers leak alleged partial Facebook marketplace database, 11 February 2024
- Bleeping Computer, Ongoing Microsoft Azure account hijacking campaign targets executives, 12 February 2024
- UNIT 42, Diving into glupteba's UEFI bootkit, 12 February 2024

- The Hacker News, Rhysida ransomware cracked, free decryption tool released, 12 February 2024
- The New Yorker, Avoiding the disinformation trap, 12 February 2024
- Eurojust, Non-Fungible Tokens and Intellectual Property Rights: Can the use of NTFs lead to IP infringements?, 13 February 2024
- Eurojust, Involvement of the Office of the Prosecutor of the International Criminal Court in joint investigation teams, 13 February 2024
- World Economic Forum, Why cybercrime spikes in times of global crisis, 13 February 2024
- We live security, The art of digital sleuthing: How digital forensics unlocks the truth, 14 February 2024
- 60 msc, Munich Security Report 2024, February 2024

Upcoming events

- 15 February 2024, C-PROC/PERU, (online), Third anniversary of the Cybercrime Unit of the Public Ministry of Peru, GLACY-e
- 16 February 2024, C-PROC/LIBYA, (online), Co-ordination meeting with representatives of the European Union Delegation to Libya to discuss synergies and co-operation plans under CyberSouth+
- 19 February-8 March 2024, C-PROC/TUNISIA, (in-person), Translation into English and French of the Tunisian Guide on electronic evidence
- 19-23 February 2024, C-PROC/FIJI, (in-person), E-evidence training first responders' course (national pilot course), GLACY-e
- 19-23 Feb 2024, C-PROC/GLOBAL, (in-person), Digital Security Challenge 2024, GLACY-e
- 20 February 2024, C-PROC/LEBANON, (online), Meeting with representatives from the European Commission Directorate-General for Justice and Consumer Protection, the Council of Europe Data Protection Unit and the Council of Europe Office in Tunis to co-ordinate joint activities on data protection in Lebanon
- 20 February 2024, C-PROC/EGYPT, (online), Meeting with EU Delegation to the Arab Republic of Egypt to discuss future co-operation under CyberSouth+
- 22-23 February 2024, C-PROC/GAMBIA, (online), Advisory mission on the Evidence Bill, GLACY+
- 26 Feb-8 March 2024, C-PROC/BRAZIL, (online), Introductory course for national trainers (prosecutors), GLACY-e
- 26 Feb-8 March 2024, C-PROC/BRAZIL, (online), Adult training methodology for national trainers (prosecutors), GLACY-e
- 29 February 2024, C-PROC, (online), First webinar of the fourth practitioner-to-practitioner series (under the framework of the International Network of Judicial Trainers), GLACY-e
- by February 2024, C-PROC/ ECUADOR, (online), Development of a specialised module on gendered aspects of cybercrime in Ecuador, GLACY-e
- February 2024, C-PROC, (*online*), further developments of the Octopus platform, Octopus
- February 2024, C-PROC, (*online*), further developments of the CYBOX platform, Octopus
- February 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