Cybercrime Digest

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

1 - 15 October 2023

Source: Council of Europe

Date: 04 October 2023

Rwanda and São Tomé and Príncipe invited to join the Convention on Cybercrime

"On 4 October, Rwanda and São Tomé and Príncipe were invited to accede to the Budapest Convention on Cybercrime. This invitation to accede is valid for five years from its adoption. African countries are demonstrating an increasing commitment to co-operate on cybercrime and to make use of the framework of the Convention on Cybercrime for this purpose. The Council of Europe will now support Rwanda and São Tomé and Príncipe through capacity building activities." READ MORE

Source: Council of Europe

Date: 06 October 2023

Kyoto: Council of Europe at the Internet Governance Forum

"The Council of Europe is participating in the 18th UN Internet Governance Forum (IGF) hosted by the government of Japan from 8 to 12 October in Kyoto, Japan, under the theme "The Internet We Want - Empowering All People". In addition to engaging in the general discussions, the Council of Europe will organise or co-organise several events, mainly focusing on artificial intelligence (AI), the use of electronic evidence and open-source intelligence (OSINT) in the context of war crimes and human rights violations, as well as emerging technologies such as the metaverse." READ MORE

RELATED ARTICLES:

Council of Europe, Le Secrétaire général adjoint au FGI : « Tirons parti des avantages de l'IA sans sacrifier nos valeurs », 9 October 2023

Dig Watch, IGF 2023 main session on the urgent need for cybersecurity, trust, and online safety, 10 October 2023

Source: International Committee of the Red Cross

Date: 05 October 2023

8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them

"As digital technology is changing how militaries conduct war, a worrying trend has emerged in which a growing number of civilians become involved in armed conflicts through digital means. Sitting at some distance from physical hostilities, including outside the countries at war, civilians – including hacktivists, to cyber security professionals, 'white hat', 'black hat' and 'patriotic' hackers – are conducting a range of cyber operations against their 'enemy'. Some have described civilians as 'first choice cyberwarriors' because the 'vast majority of expertise in cyber (defence) lies with the private (or civilian) sector'." READ MORE

RELATED ARTICLE:

Security week, Red Cross publishes Rules of engagement for hacktivists during war, 5 October 2023

Source: Politico

Date: 15 October 2023

How hackers piled onto the Israeli-Hamas conflict

“Hackers sympathetic to Hamas are working to make the Israel-Gaza conflict the next front of cyberwarfare. Hacking groups with links to countries including Iran and Russia have launched a series of cyberattacks and online campaigns against Israel over the past week, some that may have even occurred in the runup to the Oct. 7 strike by Hamas. […] It’s unclear how far and deep the cyberattacks went. But the online campaigns show an effort to bolster the physical onslaught with a digital offensive, potentially looking to replicate the way Russia and sympathetic hacktivists buffeted Ukraine with cyber strikes in the first days of that war.” READ MORE

RELATED ARTICLES:

The Record, European Commission demands X account for disinformation in wake of Hamas attacks, 12 October 2023

The Washington Post, Hamas vows to broadcast hostage executions. Tech firms can’t stop them, 12 October 2023

The New York Times, False claims around Israel attacks include recycled videos and a game clip, 12 October 2023

Source: Europol

Date: 06 October 2023

EC3 Cybercrime Conference 2023

“Europol will host the 2nd EC3 Cybercrime Conference on 18 and 19 October 2023. The theme for this year is “10 years of joint support to operations against cybercrime – building tomorrow's partnerships". Since its establishment in 2013, EC3 has made a significant contribution to the fight against cybercrime and it has been involved in many high-profile operations and hundreds of operational-support deployments.” READ MORE

Source: EURACTIV

Date: 15 October 2023

UN cybercrime treaty: A menace in the making

“[…] Governments are meeting in Vienna beginning October 19 to negotiate a global treaty on cybercrime. But instead of sticking to the task at hand – fostering global expertise and cooperation in cybercrime – the proposed treaty seeks expansive powers to investigate virtually any imaginable criminal offence, even if no technology is involved at all. This misguided approach will facilitate cross-border repression. And it will make it more difficult to investigate actual cybercrime.” READ MORE

Source: European Commission

Date: 12 October 2023

The Commission sends request for information to X under the Digital Services Act*

“Today the European Commission services formally sent X a request for information under the Digital Services Act (DSA). This request follows indications received by the Commission services of the alleged spreading of illegal content and disinformation, in particular the spreading of terrorist and violent content and hate speech. The request addresses compliance with other provisions of the DSA as well.” READ MORE

Source: ICANN

Date: 05 October 2023

ICANN Contracted Parties Set to Vote on Proposed DNS Abuse Amendments

"[…] The opening of the voting period is a significant milestone in this important initiative to enhance efforts to combat DNS Abuse. Over the past several years a variety of constituents, including governments and review teams, have been calling on ICANN and the community to do more to combat DNS Abuse. In response, in late 2022, contracted parties (CPs) proposed to the ICANN organization the idea of developing specific improvements to the 2013 Registrar Accreditation Agreement and Base gTLD Registry Agreement focused on DNS Abuse, which led to the proposed amendments. These proposed amendments are an important building block to mitigating DNS Abuse and position the community well for further policy discussions on what additional steps can be taken to combat DNS Abuse even more effectively." READ MORE

Source: Eucrim

Date: 11 October 2023

Electronic Evidence Collection in Cases of the European Public Prosecutor's Office

"The European Public Prosecutor's Office (EPPO) is the independent public prosecution office of the European Union responsible for investigating, prosecuting, and bringing to judgment crimes against the financial interests of the EU.1 Like for any other national criminal justice authority, EPPO's success in investigating and prosecuting crime relies on the lawful, effective, and efficient collection of evidence. The perpetrators of offences falling within EPPO's jurisdiction often make use of the Internet and information and communication technologies (ICTs) in the course of organising and committing their crimes, laundering the crime proceeds, or hiding the traces of their offences." READ MORE

Source: Mediavenir

Date: 13 October 2023

Comment pister les mouvements des acteurs malveillants grâce aux données historiques WHOIS

"Qui aurait cru que derrière une simple adresse de site web pourrait se cacher toute une histoire, riche en détails et en connexions ? Il ne s'agit pas de magie, mais d'une science méticuleuse. Les données historiques WHOIS ont transformé la façon dont nous traquons les acteurs malveillants sur le web." READ MORE

Source: Europol

Date: 12 October 2023

Investigations Targeted: human traffickers luring victims online

"The Netherlands, supported by Europol, coordinated a three-day long operational action targeting online criminal activities that enable human trafficking. The 2023 Hackathon took place from 18 to 22 September in Apeldoorn, the Netherlands, and involved 85 experts: law enforcement officers from 26 countries (22 EU Member States and 4 third countries) as well as representatives from the European Labour Authority, CEPOL, INTERPOL, the OSCE and the International Justice Mission." READ MORE

Source: OSCE

Date: 04 October 2023

OSCE Media Freedom Representative launches new guidelines for monitoring online violence against female journalists

"Today, OSCE Representative on Freedom of the Media Teresa Ribeiro launched the new Guidelines for monitoring online violence against female journalists at the Warsaw Human Dimension Conference. The Guidelines provide a systematic monitoring and reporting system aiming to better protect women journalists and prevent online violence from escalating." READ MORE

Source: The Hacker News

Date: 10 October 2023

New Report: Child sexual abuse content and online risks to children on the rise

"Certain online risks to children are on the rise, according to a recent report from Thorn, a technology nonprofit whose mission is to build technology to defend children from sexual abuse. Research shared in the Emerging Online Trends in Child Sexual Abuse 2023 report, indicates that minors are increasingly taking and sharing sexual images of themselves. This activity may occur consensually or coercively, as youth also report an increase in risky online interactions with adults." READ MORE

RELATED ARTICLE:

Safer, Emerging online trends in child sexual abuse 2023 report

Source: United Nation

Date: 02 October 2023

With criminal groups using sophisticated technologies to ply their wares, Third Committee Stresses urgent need to collectively combat transnational crime

"Organized criminal groups use technology in every step of their process, the Third Committee (Social, Humanitarian and Cultural) heard today, as delegates highlighted the many scourges stemming from human trafficking and outlined ways to prevent crime and combat the illicit trafficking of drugs, corruption, terrorism and organized crime. Delphine Schantz, representative of the New York Liaison Office, United Nations Office on Drugs and Crime (UNODC), said the rapid expansion of online connectivity without a parallel development of risk management measures at legal and policy levels has increased the risk of cyberdependent and cyberenabled criminal activities." READ MORE

Source: Europol

Date: 05 October 2023

Europol and TikTok collaborate to bolster efforts against terrorist content

"On 28 September, a large-scale voluntary Referral Action Day between TikTok, Europol's European Counter Terrorism Centre (ECTC) and 11 countries took place targeting suspected terrorist and violent extremist content online. In collaboration with the video sharing platform TikTok, investigators from the participating countries, together with the ECTC's European Union Internet Referral Unit (EU IRU), performed an exercise to detect material glorifying past terrorist attacks or terrorist perpetrators." READ MORE

Source: Daily Dot

Date: 02 October 2023

Furry hackers claim to have breached NATO, stolen 3,000 files

"The hacking group SiegedSec announced on Monday that it has leaked what are claimed to be more than 3,000 files from the North American Treaty Organization (NATO). […] The hacking group SiegedSec announced on Monday that it has leaked what are claimed to be more than 3,000 files from the North American Treaty Organization (NATO)." READ MORE

RELATED ARTICLE:

Reuters, NATO 'actively addressing' alleged cyberattack affecting some websites, 3 October 2023

Source: We live security

Date: 05 October 2023

Operation Jacana: Foundling hobbits in Guyana

"In February 2023, ESET researchers detected a spearphishing campaign targeting a governmental entity in Guyana. While we haven't been able to link the campaign, which we named Operation Jacana, to any specific APT group, we believe with medium confidence that a China-aligned threat group is behind this incident. In the attack, the operators used a previously undocumented C++ backdoor that can exfiltrate files, manipulate Windows registry keys, execute CMD commands, and more." READ MORE

RELATED ARTICLE:

The Record, Suspected China-linked hackers target Guyana government with new backdoor, 5 October 2023

Source: The Record

Date: 06 October 2023

Rhysida ransomware gang claims attacks on governments in Portugal, Dominican Republic

"A notorious ransomware gang has claimed attacks against two government institutions this week, both of which confirmed they faced a range of issues due to the incidents. The city of Gondomar – a suburb about 20 minutes away from the Portuguese city of Porto – said on September 27 that it was the target of a cyberattack that forced officials to take systems offline and contact the country's National Cybersecurity Center and the National Data Protection Commission and local law enforcement." READ MORE

Source: Gestion

Date: 05 October 2023

Costa Rica: Futuro del 5G será analizado por expertos en medio de polémica en Costa Rica

"El futuro tecnológico del 5G será analizado por expertos en medio de la polémica en Costa Rica por la exclusión de participar en contratos para el desarrollo de esta tecnología a países que no hayan firmado el Convenio de Budapest sobre ciberseguridad, entre los cuales se encuentra China. En el foro organizado por EFE Diálogos titulado: "Ciberseguridad y 5G. La innovación marcará el futuro de Centroamérica" se abordarán los desafíos a los que se enfrenta Costa Rica y otros países de la región durante la introducción de la tecnología 5G, que será decisiva para países punteros en innovación digital y conectividad." READ MORE

Source: The Tico Times

Date: 02 October 2023

Pioneering a Blueprint to combat Online Hate Speech in Costa Rica

"Costa Rica is pioneering a bold new strategy to combat the alarming rise of online hate speech in Latin America. As highlighted by Faustina Torres, a member of the Bribri indigenous community, discrimination and invisibility of minority groups persists in Costa Rican society. To proactively foster inclusive digital spaces, Costa Rica is developing the region's first national strategy against online hate speech and discrimination, with support from the United Nations." READ MORE

Source: INTERPOL

Date: 05 October 2023

INTERPOL conference: Global security hinges on a safer Africa

"Police leaders from Africa have voted to adopt a series of far-reaching recommendations to boost the exchange of police data within the region. With the amount of data that countries across the region share through INTERPOL systems increasing by 7 per cent in the past year, even greater information sharing within and beyond Africa is recognized as a necessary condition to effectively address global crime threats." READ MORE

RELATED ARTICLES:

INTERPOL, INTERPOL conference calls for a common security agenda for a safer Africa, 3 October 2023

Source: Reuters

Date: 05 October 2023

Senegal seeks regulation deal with TikTok after ban

"Senegalese authorities on Thursday refused to lift a ban on social media app TikTok as they demanded that the company sign an agreement that would allow the creation of a mechanism to remove accounts. "For the time being, the restriction is being maintained pending the conclusion of a comprehensive written agreement," communications minister Moussa Bocar Thiam told a press conference, adding that authorities were in discussions with TikTok." READ MORE

Source: LOME ACTU

Date: 10 October 2023

Cybercriminalité : La police nationale arrête 13 Nigérians à Lomé

"La police togolaise a arrêté un groupe de 13 cybercriminels nigérians à Lomé, spécialisés dans les escroqueries en ligne. Ces derniers crées de faux profils sur les réseaux sociaux pour établir des relations amoureuses frauduleuses. Ils sont doués pour extorquer d'importantes sommes d'argent à leurs victimes, communément appelées "arnaques amoureuses par chat". Lors de leur arrestation, plusieurs dispositifs numériques ont été saisis, fournissant des preuves cruciales aux autorités. En outre, deux autres voleurs ont également été placés en garde à vue, dont un individu qui était recherché pour avoir volé des objets de valeur dans des voitures garées en brisant les vitres." READ MORE

Source: All Africa

Date: 12 October 2023

Tanzania: Rukwa spotted as cybercrime hotspot

"Rukwa Region is reported to lead in the country for allegedly committing cybercrime through telecom handsets, according to the Tanzania Communications Regulatory Authority (TCRA). The TRCA Manager for Southern Highland Zone Office, Engineer Asijile John said between April and June this year, a total of 8,991of telcom handset' SIM cards were identified for being associated with multiple criminal acts in Rukwa Region." READ MORE

Source: Africa News

Date: 03 October 2023

Kenya hit by record 860m cyber-attacks in a year

"Kenya has witnessed an alarming surge in cyberattacks, with a staggering 860 million incidents recorded in the past year, according to the country's communications regulator. The regulator has expressed concerns over the escalating frequency, sophistication, and scale of these cyber threats, particularly targeting Kenya's critical information infrastructure. To put this into perspective, back in 2017, Kenya faced 7.7 million cyberattacks, highlighting the significant increase over the past four years." READ MORE

Source: rfi

Date: 05 October 2023

Loi sur la cybercriminalité: «Elle va faire de la Jordanie le royaume du silence !»

"En Jordanie, la loi sur la cybercriminalité vient d'entrer en vigueur, ce qui inquiète la société civile. Pour le gouvernement, il s'agit de lutter plus efficacement contre les fausses informations et la diffamation en ligne. Pour ses détracteurs, elle muselle la liberté d'expression. À Amman, journalistes et militants sont très inquiets. Dans les rédactions des médias indépendants, la nouvelle loi est particulièrement décriée." READ MORE

Source: The Hacker News

Date: 09 October 2023

Gaza-Linked cyber threat actor targets Israeli energy and defense sectors

"A Gaza-based threat actor has been linked to a series of cyber attacks aimed at Israeli private-sector energy, defense, and telecommunications organizations. Microsoft, which revealed details of the activity in its fourth annual Digital Defense Report, is tracking the campaign under the name Storm-1133. […] Targets of the campaign included organizations in the Israeli energy and defense sectors and entities loyal to Fatah, a Palestinian nationalist and social democratic political party headquartered in the West Bank region." READ MORE

RELATED ARTICLE:

Hack Read, Hacktivists Trageting Critical ICS Infrastructure in Israel and Palestine, 10 October 2023

Security Affairs, #OPISRAEL, #FREEPALESTINE & #OPSAUDIARABIA – how cyber actors capitalize on war actions via PSY-OPS, 11 October 2023

NBC News, Gaza Strip experiencing internet outages and electricity cuts after bombings, 9 October 2023

Source: Reuters

Date: 07 October 2023

India tells X, YouTube, Telegram to remove any child sexual abuse material

“India has sent notices to social media platforms X, formerly known as Twitter, YouTube (GOOGL.O) and Telegram asking them to ensure there is no child sexual abuse material on their platforms, the government said on Friday. The companies could be stripped of their protection from legal liability if they don't comply, the government said in a statement. The notices, sent by the Ministry of Electronics and Information Technology (MEITY), emphasised the importance of prompt and permanent removal of any child sexual abuse material on the platforms.” READ MORE

Source: The Record

Date: 10 October 2023

Nation-state hacker group targeting Taiwan, US, Vietnam and Pacific Islands

“A previously unknown government-backed hacking group is targeting organizations in the manufacturing, IT, and biomedical sectors across Taiwan, Vietnam, the U.S. and an unnamed Pacific Island, according to new research from Symantec. The researchers are tracking the group under the name “Grayling” and said in a report released Tuesday that it is using custom-made malware as well as publicly available tools to attack its targets.” READ MORE

RELATED REPORT:

Symantec, Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan, 10 October 2023

Source: Bloomberg

Date: 09 October 2023

Hacked Philippine Health Insurer didn’t have cyber protection software

“The Philippines’ state health insurer didn’t have cyber protection software when hackers attacked its computers, giving criminals access to the data of millions of its citizens and triggering calls for an extensive cybersecurity audit. While the full extent of the breach has yet to be determined, the Philippine Health Insurance Corp. has warned its over 36 million members — around a third of the country’s population — that their data may have been compromised.” READ MORE

Source: Reuters

Date: 12 October 2023

Malaysia says TikTok fails to fully comply with local laws

“TikTok has not done enough to curb defamatory or misleading content in Malaysia, the communications minister said on Thursday, adding that the short video application had also failed to comply with several, unspecified local laws. […] Earlier this year, the Malaysian government said it would take legal action against Facebook parent company Meta (META.O) for violating the Communications and Multimedia Act, but dropped the plan after meetings with the company.” READ MORE

Source: Dig Watch

Date: 11 October 2023

ASEAN's innovative AI guide shifts focus, countering EU's regulatory efforts

"In a move that diverges from the European Union's ambitions for unified global AI regulations, Southeast Asian nations are adopting a business-friendly stance towards AI governance. A confidential draft of the Association of Southeast Asian Nations (ASEAN) 'guide to AI ethics and governance' has been reviewed by Reuters, with the document emphasising cultural differences and avoiding strict risk categories. Unlike the EU's AI Act, the ASEAN guide encourages companies to consider cultural diversity and does not impose specific risk categories." READ MORE

RELATED ARTICLES:

Asia Times, ASEAN, EU should work more closely tackling maritime cybercrime, 6 October 2023

Nikkei Asia, Japan, U.S., EU hold cyber defense drill with India, ASEAN support, 12 October 2023

Source: The New York Times

Date: 05 October 2023

Indonesia: TikTok forced to close shopping feature in its second-largest market

"Indonesia was one of the first countries where TikTok launched TikTok Shop, betting on the app's potential to become a successful retail platform for the company's second-largest user base. Now, the country has become the first to block the feature." READ MORE

Source: IT News

Date: 12 October 2023

Australia: National cyber security coordinator warns schools becoming targets

"Australia's national cyber security coordinator has warned that schools may be the next major target of ransomware groups. Speaking at a NAB-run seminar, Air Marshal Darren Goldie said that schools were already being targeted in the United States, and this could expand to Australia as well. "Amidst growing ransomware attacks, schools are becoming more prominent targets," he said, according to a NAB blog post." READ MORE

Source: The Fiji Times

Date: 03 October 2023

Fiji: Inaugural Pacific cyber capacity conference underway in Nadi

"Fiji's comprehensive cyber ecosystem strategy, focusing on telecommunications, equitable connectivity, digital infrastructure, and cybercrime resilience was highlighted at the inaugural Pacific Cyber Capacity Building and Coordination Conference this morning by the Deputy Prime Minister, Minister for Trade, Cooperatives, and Small and Medium Enterprises, and Communications Manoa Kamikamica at the Sheraton Hotel in Nadi. The first-of-its-kind event is a collaboration between the Partners in the Blue Pacific (PBP), the Oceania Cyber Security Centre (OCSC), and the Global Forum on Cyber Expertise (GFCE) Pacific Hub." READ MORE

Source: ABC News

Date: 06 October 2023

Australia: Home Affairs and Immigration websites hit by denial-of-service cyber attacks

"People have not been able to access visa and citizenship applications online following an attack on the Home Affairs website. The Department of Home Affairs said it was first made aware of the distributed denial-of-service (DDoS) attack overnight and an investigation had been launched." READ MORE

Source: The defense post

Date: 10 October 2023

Ukraine military opens new cyber defense training facility

"Ukraine has formally opened a new cyber classroom designed to train military specialists to effectively fend off sophisticated cyberattacks. Built with support from Estonia, the cyber classroom contains 15 workstations and necessary equipment to support cyber-related exercises. According to EU foreign policy chief Josep Borrell, the opening reflects the bloc's commitment to supporting Kyiv against a wide variety of Russian attacks." READ MORE

Source: Cybernews

Date: 04 October 2023

Russia mistakenly doxxes its own secret bases and spies

"A relatively obscure website of the Moscow City Hall has given away a list of "special consumers" on the Russian electricity grid. It includes facilities maintained by the country's military and security agencies. Of course, the information was never supposed to become public. But the Dossier Center, a non-profit investigative project, says in an extensive report that the detailed 434-page document containing the addresses was accidentally leaked online." READ MORE

Source: Council of Europe

Date: 09 October 2023

Moldovan lawyers start training on the Council of Europe HELP online course on Cybercrime and Electronic Evidence

"Over 80 lawyers from the Republic of Moldova are enrolled in the first HELP course on Cybercrime and Electronic Evidence launched in the Republic of Moldova, in cooperation with the Center for the training of Lawyers. The online launch event was held on 9 October 2023. The group was welcomed by Vladimir Palamarciuc, HELP Info Point for Moldova." READ MORE

Source: Bloomberg

Date: 04 October 2023

Deepfakes in Slovakia preview how AI will change the face of elections

"[…] Something didn't add up in an alleged conversation between Progressive Slovakia's leader, Michal Simecka, and a local journalist that circulated in the run-up to Slovakia's elections on Saturday. The speech was stilted and their voices flat even as the leader of the country's main pro-European party seemed to slag local voters, discuss buying votes from the Roma minority and joke about child pornography." READ MORE

Source: Reuters

Date: 06 October 2023

UNESCO, Dutch launch project to prepare for AI supervision

"The Netherlands and the U.N. on Thursday launched a project to help prepare Europe's national agencies to supervise artificial intelligence (AI). The project, undertaken with support of the European Commission, comes ahead of the passage of the AI Act, the broad legislation that is expected to govern AI use in Europe. In the project, The United Nations' Educational, Scientific and Cultural Organization (UNESCO) will be assembling information about how European countries are currently supervising AI and putting together a list of "best practices" recommendations." READ MORE

Source: VOA

Date: 02 October 2023

Threat of US Government shutdown fuels concerns about cyber vulnerabilities

"As the U.S. government seemed headed for a possible shutdown last week, cybersecurity firms began picking up on an alarming trend: a spike in cyberattacks targeting government agencies and the U.S. defense industry. It has some analysts concerned that U.S. adversaries and criminal hackers might have been preparing to take advantage of weaker-than-usual cybersecurity if lawmakers had not been able to reach a deal to keep U.S. agencies open past September 30." READ MORE

Source: The Record

Date: 10 October 2023

New technique leads to largest DDoS attacks ever, Google and Amazon say

"Amazon, Google and Cloudflare said they detected the largest distributed denial-of-service (DDoS) attacks on record in August due to a newly discovered vulnerability. The companies explained on Tuesday morning that a bug tracked as CVE-2023-44487 allowed threat actors a fresh angle for overwhelming websites with a flood of traffic, making them temporarily unavailable to users. Exploitation of the vulnerability is known as an HTTP/2 Rapid Reset Attack. The issue affects HTTP/2 protocol — a pivotal piece of Internet infrastructure that governs how most websites operate. The attacks have not been attributed to any known hacking group." READ MORE

Source: The interpreter

Date: 03 October 2023

Glitch in the code: Google, Meta, and the fight over news in Canada and Australia

"This year, Canada enacted Bill C.18, The Online News Act. The rather perfunctory name for the legislation belies the massive change it embodies. That law would require digital platforms such as Google and Meta to pay news media outlets to host links to their articles. Google and Meta have both strongly opposed the Bill, with Meta turning off news services for Canadian users in the midst of severe wildfires. Australians watching this stoush unfold will have an eerie sense of deja vu." READ MORE

Latest reports

- LinkedIn, The multifaceted role of digital forensics in cybersecurity and law enforcement, 2 October 2023
- Websiterating, Plus de 50 statistiques, faits et tendances sur la cybersécurité pour 2023, 2 October 2023
- Silicon Angle, Report: Over half of phishing emails now use obfuscation tactics to avoid detection, 2 October 2023
- Krebs on Security, Don't let zombie zoom links drag you down, 2 October 2023
- Sekoia Blog, Active Lycantrox infrastructure illumination, 2 October 2023
- The Hacker News, LUCR-3: Scattered Spider Getting SaaS-y in the Cloud, 2 October 2023
- Security Affairs, National Logistics Portal (NLP) data leak: seaports in India were left vulnerable to takeover by hackers, 2 October 2023
- Rediff, 10 Districts = 80% Of Cybercrime, 4 October 2023
- Bitdefender, A deep dive into stream-jacking attacks on YouTube and why they're so popular, 4 October 2023
- The Hacker News, Looney Tunables: New Linux Flaw Enables Privilege Escalation on Major Distributions, 4 October 2023
- Bleeping Computer, Researchers warn of 100,000 industrial control systems exposed online, 4 October 2023
- LinkedIn, The 3 biggest mistakes investigators make with digital evidence, 5 October 2023
- CISA, Joint advisory on top cyber misconfigurations highlights urgency for software manufacturers to incorporate secure by design principles, 5 October 2023
- ElectricIQ, Chinese state-sponsored cyber espionage activity targeting semiconductor industry in East Asia, 5 October 2023
- Elliptic, The State of Cross-chain Crime 2023, 5 October 2023
- San Francisco Chronicle, Why are there so many images of child abuse stored on iCloud? Because Apple allows it, 8 October 2023
- FORTINET, IZ1H9 Campaign Enhances Its Arsenal with Scores of Exploits, 9 October 2023
- Bleeping Computer, HelloKitty ransomware source code leaked on hacking forum, 9 October 2023
- Check Point, R2R stomping – are you ready to run?, 9 October 2023
- Akamai, The art of concealment: a new magecart campaign that's abusing 404 Pages, 9 October 2023
- BW Security World, How to report cybercrime in India? Step to step guide, 10 October 2023
- Mandiant, Assessed cyber structure and alignments of North Korea in 2023, 10 October 2023
- Security Week, Microsoft fixes exploited zero-days in WordPad, Skype for Business, 10 October 2023
- Google Cloud, How it works: The novel HTTP/2 'Rapid Reset' DDoS attack, 10 October 2023
- Mondag, Switzerland: Anti-Money Laundering Comparative Guide, 10 October 2023
- UK Government, Home Office annual report and accounts 2022 to 2023 (accessible), 11 October 2023

- Check Point Research, Stayin' alive – targeted attacks against telecoms and government ministries in Asia, 11 October 2023
- Jus Corpus Law Journal, Impact of AI on electronic evidence, 11 October 2023
- CISA, FBI and CISA release update on AvosLocker Advisory, 11 October 2023
- Bleeping Computer, Microsoft: State hackers exploiting Confluence zero-day since September, 11 October 2023
- Cofese, Resurgence of LinkedIn Smart Links Identified in Sizable Credential Phishing Campaign, 11 October 2023
- Phylum, Phylum Discovers SeroXen RAT in Typosquatted NuGet Package, 12 October 2023
- OSCE, Ensuring Human Rights Compliance in Cybercrime Investigations, 13 October 2023
- CISA, CISA and International Partners--Starting a Global Movement to Secure Our World, 13 October 2023
- Bleeping Computer, AI algorithm detects MitM attacks on unmanned military vehicles, 14 October 2023
- Security Affairs, The ALPHV Ransomware Gang stole 5TB of data from the Morrison community hospital, 15 October 2023
- Freedom House, The repressive power of Artificial Intelligence, October 2023
- Microsoft, Microsoft Digital Defense Report 2023, October 2023

Upcoming events

- 16-17 October 2023, C-PROC/LISBON, *(in person),* Contribution to the Lisbon Forum of the North-South Centre on Human Rights, Environment and Economic Crimes: Youth at the forefront, CyberSouth
- 16–18 October 2023, C-PROC/NORTH MACEDONIA, *(in person),* Final assessment mission, iPROCEEDS-2
- 16–19 October 2023, C-PROC/FRANCE*, (in person),* ETSI Cyber Security Conference (BiH), iPROCEEDS-2
- 16-28 October 2023, C-PROC/JORDAN, *(online),* Meetings with relevant national institutions of Lebanon and Jordan, to assess progresses to fight cybercrime, in the framework of the CyberSouth project, CyberSouth
- 17-19 October 2023, C-PROC/MALAWI, *(in person),* Advisory mission on legislation, GLACY+
- 17 October 2023, C-PROC/BELGIUM, *(in person),* Roundtable with LAC Embassies on the capacity building options (organized by EU CyberNet), GLACY+
- 17-27 October 2023, C-PROC/ITALY, *(in person),* International Advanced Training Institute for the prevention of and the fight against organized crime (support for hub countries to attend specialized courses), GLACY+
- 17-19 October 2023, C-PROC/SINGAPORE, *(in person),* 6th ASEAN Cybercrime prosecutors' Roundtable meeting and Singapore international cyber week (support for hub countries to attend specialised meetings), GLACY+
- 18 October 2023, C-PROC/BELGIUM, *(in person*), EU CyberNet Stakeholder Community Day (organized by EU CyberNet), GLACY+
- 18 October 2023, C-PROC/HELP/HUNGARY, (*in person*), Launch of the HELP Course on Cybercrime for Hungarian prosecutors, Budapest, Hungary, Octopus
- 18-19 October 2023, C-PROC/EUROPOL/THE NETHERLANDS, (*in person*), Support the participation of delegates from a selected number of countries to Europol Cybercrime Conference, CyberEast, Octopus, iPROCEEDS-2, CyberSouth, GLACY+
- 19 October 2023, C-PROC/HELP/IRELAND (*in person*), Cross-border launch of the HELP Course on Cybercrime for Irish lawyers and legal professionals, Octopus
- 20 October 2023, C-PROC/THE NETHERLANDS, (*in person*), Meeting of the 24/7 Network of Contact Points of the Budapest Convention, iPROCEEDS-2, Octopus, CyberEast, CyberSouth, GLACY+
- 20 October 2023, C-PROC/THE NETHERLANDS, *(in person),* Workshops with European Commission Directive 977/2023 and International Association of Prosecutors, iPROCEEDS-2
- 23–27 October 2023, C-PROC/GEORGIA, *(in person),* International simulation exercises for cybersecurity and cybercrime communities, iPROCEEDS-2, CyberEast
- 23-27 October 2023, C-PROC/RWANDA, *(in person*), Legislative drafting workshop - part 2, GLACY+
- 24-26 October 2023, C-PROC/GHANA, *(in person*), Support for national delivery - Introductory course on cybercrime and electronic evidence for judges and prosecutors, GLACY+
- 24–25 October 2023, C-PROC/MONTENEGRO, *(in person),* Final assessment mission, iPROCEEDS-2

- 26 October 2023, C-PROC, *(online)*, INNJT Practitioners-to-practitioners workshop on cryptocurrencies, GLACY+, Octopus, CyberEast, iPROCEEDS-2, CyberSouth,
- October 2023, C-PROC, *(online)*, maintaining cyberviolence portal, 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