Cybercrime Digest

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

01 - 15 March 2024

Source: Tunisie Numérique

Date: 08 March 2024

La Tunisie adhère officiellement à la Convention du Conseil de l'Europe sur la cybercriminalité

"La Tunisie a officiellement adhéré à la Convention du Conseil de l'Europe sur la cybercriminalité adoptée à Budapest, devenant ainsi le 70ème pays à adhérer à cette convention. […] L'adhésion de la Tunisie à cet accord vise à contribuer efficacement au soutien et à la coordination des efforts internationaux dans le domaine de la lutte contre la cybercriminalité et à atteindre une efficacité suffisante dans la préservation des droits des personnes et des victimes de la cybercriminalité, car l'accord permettra aux structures nationales concernées par la lutte contre la criminalité liée à les systèmes d'information et de communication, de bénéficier de l'expertise, de la formation et des procédures juridiques qui, notamment au niveau de l'échange d'informations entre les États membres, dans le but de prévenir, détecter et dissuader ces crimes." READ MORE

RELATED ARTICLES:

Council of Europe, Tunisia becomes the 70th Party to Convention on Cybercrime, 08 March 2024

Source: The Record

Date: 06 March 2024

EU strikes political agreement on Cyber Solidarity Act in wake of Russian attacks

"The Cyber Solidarity Act was proposed last year, featuring three pillars intended to address "the urgent need" for the bloc to be able to "detect, prepare for and respond to cybersecurity threats and incidents." […] According to the Commission, despite the potential cross-border impacts of cyber incidents there is currently a "limited" amount of relevant information sharing. […] the Cyber Solidarity Act will create and fund a federated network of national security operations centers called the European Cyber Shield […]." READ MORE

Source: Council of Europe

Date: 15 March 2024

Artificial Intelligence, Human Rights, Democracy and the Rule of Law Framework Convention

""While this treaty has been elaborated by the Council of Europe with like-minded international partners, it will be a global instrument, open to the world. After its adoption by our Committee of Ministers in the coming weeks, countries from all over the world will be eligible to join it and meet the high ethical standards it sets. The Framework convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law has been finalised yesterday by the Council of Europe Committee on Artificial Intelligence. The draft text will be referred to the Committee of Ministers for adoption and opened for signature at a later stage." READ MORE

Source: European Parliament

Date: 13 March 2024

Artificial Intelligence Act: MEPs adopt landmark law

"On Wednesday, Parliament approved the Artificial Intelligence Act that ensures safety and compliance with fundamental rights, while boosting innovation. […] It aims to protect fundamental rights, democracy, the rule of law and environmental sustainability from high-risk AI, while boosting innovation and establishing Europe as a leader in the field. The regulation establishes obligations for AI based on its potential risks and level of impact. […] Citizens will have a right to submit complaints […]." READ MORE

Source: DigWatch

Date: 07 March 2024

Decision postponed on the Cybercrime Convention: What you should know about the latest session of the UN negotiations

"[…] The Ad Hoc Committee (AHC) was tasked with drafting a comprehensive cybercrime convention. However, as the final session started, there were no signs of significant progress: member states couldn't agree on significant issues such as the scope of the convention. […] One of the main unresolved points remains the question whether the cybercrime convention should be a traditional treaty or if it should cover all crimes committed via ICTs. This divide translated into a lengthy discussion on the name of the convention itself, as well as on Article 3 (scope of application) of the draft convention." READ MORE

Source: Europol

Date: 08 March 2024

57 men arrested for possessing and sharing over 100 000 depictions of child sexual abuse

"Europol classifies perpetrators who possess or distribute material depicting the sexual abuse of children, and simultaneously possess manuals about committing sexual abuse, as High Value Targets. They are assumed to be the most likely to physically abuse children. The 57 national investigations into the crimes committed by the arrested persons will also be a starting point for further law enforcement action, with more arrests and seizures to be expected across Europe. […] The overall ultimate strategic goal of operations such as this one is to eliminate the risk of children being sexually abused. Every child counts, and for every child saved this means a world of difference." READ MORE

Source: Asia Times

Date: 12 March 2024

Russia using Ukraine as a cyberwar testing ground

"As Russian tanks invaded Ukraine in August 2014, Russian hackers were already working on conducting cyberattacks against Ukraine, with the country distracted by what was happening politically. The war in eastern Ukraine also gave Russia-affiliated hackers the opportunity to begin launching extensive cyberattacks against Ukraine. As a result, Ukraine's situation would end up being termed "Russia's test lab" for cyberwar. […] As compared with typical ransomware, which encrypts data and demands payment for its release, NotPetya was more destructive as it masqueraded as ransomware but was designed primarily to wipe data and disrupt systems.'' READ MORE

Source: KrebsonSecurity

Date: 11 March 2024

Incognito Darknet Market Mass-Extorts Buyers, Sellers

"Borrowing from the playbook of ransomware purveyors, the darknet narcotics bazaar Incognito Market has begun extorting all of its vendors and buyers, threatening to publish cryptocurrency transaction and chat records of users who refuse to pay a fee ranging from $100 to $20,000. The bold mass extortion attempt comes just days after Incognito Market administrators reportedly pulled an "exit scam" that left users unable to withdraw millions of dollars worth of funds from the platform. […] Incognito Market says it plans to publish the entire dump of 557,000 orders and 862,000 cryptocurrency transaction IDs at the end of May." READ MORE

Source: Abnormal

Date: 07 March 2024

Key Takeaways from the 2023 FBI IC3 Report: Business Email Compromise Losses Jump to Nearly $3 Billion

"Today, the FBI Internet Crime Complaint Center (IC3) released its 2023 Internet Crime Report, which examines cybercrime trends from the prior year, providing details on total losses and the number of reported victims. The latest report revealed that business email compromise (BEC) remains a significant threat for modern enterprises, resulting in reported losses of nearly $3 billion. This represents a 7% increase over 2022's already staggering total of $2.7 billion—and a total of $14.3 billion since the IC3 began including the attack in its report in 2015." READ MORE

Source: ENISA

Date: 06 March 2024

Safeguarding EU elections amidst cybersecurity challenges

"Since the last EU elections in 2019, the elections threat landscape has evolved significantly. For instance, the rapid developments in AI including deep fakes, hacktivists-for-hire, sophistication of threat actors along with today's geopolitical context highlight the necessity to update the compendium in order to reflect the current risks and threats. […] Taking into account the diversity in the national electoral processes across the EU, the compendium provides a compilation of practical recommendations and measures to be used by the EU entities and national authorities that support elections." READ MORE

Source: Interpol

Date: 06 March 2024

Revised toolkit empowers law enforcement with responsible AI practices

"NTERPOL and UNICRI have released an updated version of the Toolkit for Responsible AI Innovation in Law Enforcement, a practical guide for law enforcement agencies on developing and deploying artificial intelligence responsibly, while respecting human rights and ethics principles. The AI Toolkit is comprised of seven distinct resources, underpinned by a comprehensive user guide, providing guidance for law enforcement executives and officers to navigate responsible AI innovation from technical foundations to organizational assessments on readiness and risk." READ MORE

Source: Eurojust

Date: 07 March 2024

Eurojust and eu-LISA discuss closer cooperation to support digitalisation of justice across Europe

"This cooperation could, for example, focus on ensuring the interoperability of EU-wide digital systems with those of national authorities, the implementation of the Joint Investigation Teams Collaboration Platform and the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), as well as the possible use of artificial intelligence (AI) in the field of judicial cooperation. […] In addition, the development by eu-LISA of a specific collaboration platform for joint investigation teams (JITs CP) will provide a secure and efficient tool for the exchange of information between the different cross-border teams, which together with the vital support provided by Eurojust, will concretely streamline their work." READ MORE

Source: The Hacker News

Date: 09 March 2024

Microsoft Confirms Russian Hackers Stole Source Code, Some Customer Secrets

"Microsoft on Friday revealed that the Kremlin-backed threat actor known as Midnight Blizzard (aka APT29 or Cozy Bear) managed to gain access to some of its source code repositories and internal systems following a hack that came to light in January 2024. "In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access," the tech giant said.'' READ MORE

Source: FIIAP

Date: 13 March 2024

Fight against organised crime: Europe and Latin America extend their alliance to Caribbean countries

"Strengthening the rule of law and combating organised crime by promoting coordination between the 33 countries of Latin America and the Caribbean and their strategic partnership with the European Union. This is the objective of the programme presented at a high-level event in Panama City that brought together 300 representatives of justice and security institutions from Latin America, the Caribbean and the European Union, including 50 ministers and deputy ministers of justice and security, attorneys general, presidents of judicial bodies and the highest authorities of the regional bodies of the European Union, Latin America, Latin America and the Caribbean." READ MORE

Source: Council of Europe

Date: 11-13 March 2024

GLACY-e: Ecuador makes progress towards developing a national cybercrime strategy

"At the initiative of the Ministry of Interior, representatives of more than 10 national authorities have been invited to a 3-day workshop facilitated by the Ministry of Foreign Affairs and Human Mobility of Ecuador to work collaboratively on the first draft of the strategy. Participants agreed on a set of objectives covering […]: enhancing legislation and governmental capacities, preventing cybercrime targeted at citizens and institutions, addressing transnational criminal structures and improving public-private cooperation and access to e-evidence in criminal investigations." READ MORE

Source: Sinart Digital

Date: 13 March 2024

Costa Rica: Fiscalía urge reformas procesales para afrontar ciberdelitos

"[…] La cantidad de denuncias por ciberdelitos cada día son más. Y, para la Fiscalía, la única manera de detener esto sería generando reformas procesales que les facilite tanto la labor de investigación como la de obtención de prueba. Actualmente, estos delitos -que tienen una constante actualización- se persiguen con leyes que datan desde hace muchos años, lo cual repercute negativamente en el resultado final. […] Ahora se está trabajando en suscribir el Segundo Protocolo Adicional del Convenio de Budapest; sin embargo, para el fiscal, hay que generar un proyecto de ley para poner en práctica lo que allí se estipula." READ MORE

Source: Gobierno del Perú

Date: 06 March 2024

Fiscales de Latinoamérica compartirán criterios frente a desafíos que plantea la ciberdelincuencia

"Ante las constantes´ciberamenazas´contra la ciudadanía y los Estados, mediante distintos tipos de ataques y hechos delictivos a través de las tecnologías de la información y las comunicaciones (TIC), fiscales de distintos países se reunirán en un encuentro académico denominado ´Foro Regional de Fiscales Especializados en investigación en el Ciberespacio´." READ MORE

Source: Security Intelligence

Date: 13 March 2024

PixPirate: The Brazilian financial malware you can't see

"PixPirate is a sophisticated financial remote access trojan (RAT) malware that heavily utilizes anti-research techniques. This malware's infection vector is based on two malicious apps: a downloader and a droppee. Operating together, these two apps communicate with each other to execute the fraud. So far, IBM Trusteer researchers have observed this malware attacking banks in Brazil. READ MORE

RELATED ARTICLE:

Fortinet, New Banking Trojan "CHAVECLOAK" Targets Brazil, 04 March 2024

Source: Council of Europe

Date: 04 March 2024

CyberSouth+ contributes to the launch of the Rule of Law Youth Network, supported by the North-South Centre and Programme South V of the Council of Europe

"The objective of this network, which includes among others representatives from Algeria, Egypt, Jordan, Lebanon, Morocco, Palestine* and Tunisia is to increase young people awareness and ownership of human rights, rule of law and democratic standards, and promote their actions to increase their influence over on-going and future reforms and their sustainability. CyberSouth+ contributed with a presentation and discussion on cybercrime threats, on how they impact our societies and what we can do to counter them, using the tools offered by the Council of Europe Cybercrime Convention." READ MORE

Source: Digital Business Africa

Date: 06 March 2024

Cybercriminalité : Group-IB signale un nombre d'escroqueries par usurpation d'identité croissant dans la région MEA en 2023

"La région du Moyen-Orient aurait été, selon le rapport, victime d'attaques de ransomwares et le nombre de cas où leurs données ont été publiées dans des DLS a augmenté de 65 % par rapport à l'année dernière. Par ailleurs, au deuxième semestre 2023, les activités des hacktivistes se sont multipliées dans la région." READ MORE

Source: BBC

Date: 01 March 2024

Binance: Nigeria orders cryptocurrency firm to pay $10bn

"The Nigerian government says it has demanded almost $10bn (£8bn) in compensation from the cryptocurrency firm, Binance. It says Binance manipulated foreign exchange rates through currency speculation and rate-fixing, which have seen the naira lose nearly 70% of its value in recent months. [...] Nigeria is Africa's biggest economy and also one of the world's biggest cryptocurrency markets. […] Cryptocurrency transactions equivalent to about 12% of Nigeria's total income, or GDP, took place in the year to June 2023, according to Reuters news agency." READ MORE

Source: The Africa Report

Date: 07 March 2024

East Africa governments need to act on nationals trapped in Southeast Asia cyber slavery

"Ugandans, Kenyans, Ethiopians and Egyptians are among those forced into cyber-slavery scams in Myanmar and Cambodia. Governments in East Africa need to act to reduce the risks of more of their citizens being trapped in cyber slavery in Southeast Asia, Mina Chiang, director of the Humanity Research Consultancy, tells The Africa Report. […] Many of the slaves and their financial victims are Chinese. But the cyber gang masters know that the richest pickings are to be found in the English-speaking world. They have increasingly sought to lure young English speakers from areas, including East Africa, under the false promise of well-paid, legitimate employment." READ MORE

Source: Agence Ecofin

Date: 02 March 2024

L'Afrique du Sud face à une vague de ransomwares : une aubaine pour le marché de la cybersécurité

"Les pays africains, et particulièrement l'Afrique du Sud, sont confrontés depuis peu à la composante cybersécurité du fait de l'accélération de leur transformation numérique. Face à ce défi, les Etats cherchent des solutions, ce qui peut constituer une opportunité pour les entreprises africaines spécialisées dans le secteur. L'Afrique du Sud se distingue en tant que le pays africain qui fait face au plus grand nombre d'incidents de ransomwares, se classant au huitième rang mondial, selon un rapport publié par la Carnegie Endowment for International Peace en janvier 2024." READ MORE

Source: Hack Read

Date: 04 March 2024

Nepali Hacker Tops Hall of Fame by Exposing Facebook's Zero-Click Flaw

"The vulnerability was discovered in Facebook's password reset functionality. It allowed hackers to bypass the system's rate-limiting feature and subsequently check possible combinations of 6-digit numbers (from 000000 to 999999) for two hours. In his blog, Aryal revealed finding a vulnerable endpoint on Android Studio while testing Facebook versions. He received a pop-up in the password reset flow offering users to send a security code through Facebook notification. The code remained active for two hours despite incorrect inputs. […] To stay safe, users should enable two-factor authentication, use strong, unique passwords, be cautious with password reset requests, and stay updated on security threats." READ MORE

Source: IPD Forum

Date: 03 March 2024

U.N. report: North Korea financing weapons program with cybercrime

"United Nations investigators say North Korea has stolen billions of dollars in cyberattacks to fund the regime's weapons of mass destruction. The U.N. found 58 suspected North Korean cyberattacks between 2017 and 2023, valued at about $3 billion, The Associated Press (AP) reported in February 2024. Hacking groups reporting to Pyongyang's primary foreign intelligence organization continue to conduct cyberattacks, U.N. experts said. The report came just days after South Korea unveiled a new strategy to counter North Korea's cyber threats. Seoul's approach is based on the country's National Security Strategy published in June 2023 and follows the November 2023 formation of a trilateral working group with Japan and the United States to counter North Korea's increasing cyber threats." READ MORE

Source: Dark Reading

Date: 01 March 2024

Taiwan's Biggest Telco Breached by Suspected Chinese Hackers

"Taiwan's Defense Ministry is urging Chunghwa Telecom, the the island's largest telecom company, to improve its cybersecurity following a data breach that compromised government-related information. The hackers, reportedly believed to be backed by the Chinese government, made off with 1.7TB of data following the Chunghwa compromise and have put it all up for sale on the Dark Web." READ MORE

Source: Ecns

Date: 13 March 2024

China: Prosecutors take tougher stance on crime involving minors

"Chinese prosecutors are taking a tougher stance against crimes targeting minors and juvenile delinquency, which have seen steady increases in recent years, according to a white paper issued by the Supreme People's Procuratorate. […] Xian Jie, head of the top procuratorate's office for minors' affairs, highlighted the vulnerability of minors to online violence, obscenity and addiction, potentially leading them down a path of criminal activity. Additionally, some internet companies that prioritize profit over social responsibility further endanger minors and information security." READ MORE

Source: IT News

Date: 13 March 2024

Australian police link "over 11,000 cybercrime incidents" to Medibank breach

"A joint police operation targeting misuse of personal information after high-profile Australian hacks has linked "over 11,000 cybercrime incidents" to the Medibank data breach. The number is contained in a submission by Victoria Police to a federal cybercrime inquiry and appears to be the first time a measure of fallout from the incident has been disclosed. It relates to the work of 'Operation Guardian', which brings together federal, state and territory police and other organisations to […] "identify, disrupt, charge and prosecute any person seeking to exploit personally identifiable information (PII) obtained from [a] data breach."." READ MORE

Source: 9news

Date: 04 March 2024

Australia: Nearly 3500 scam websites shut down in major government swoop

"Almost 3500 scam websites have been knocked out in a major government crackdown on fraudsters looking to strip cash from Australians. The Australian Securities and Investments Commission (ASIC) wiped out thousands of websites in just six months and is in the process of taking down another 350 sites. […] The financial watchdog was pursuing investment scam and phishing websites, Longo said, "removing them from the internet before they can lure in unsuspecting consumers". ASIC was out to hammer the scammers with fines and prison sentences, he said. The watchdog secured almost $60 million in civil penalties and nine criminal convictions in the second half of 2023." READ MORE

Source: The Record

Date: 06 March 2024

Moldova warns of Russian 'hybrid attacks' ahead of presidential election

"Moldova's national intelligence agency warned Tuesday that it believes Russia plans to launch hybrid attacks against the country ahead of its upcoming elections, which will include a referendum on joining the European Union. […] According to Moldova's Intelligence and Security Service (SIS), part of Russia's strategy involves the "extensive use of social networks," such as Telegram and TikTok, to promote pro-Moscow politicians, encourage anti-government protests and incite inter-ethnic hatred." READ MORE

Source: Europol

Date: 07 March 2024

Tabletop exercise hosted by Europol to disrupt terrorist content online

"The exercise took place in the framework of the EU Internet Forum and examined the collaboration between government authorities and the tech industry to contain the viral spread of terrorist and violent extremist content online in the aftermath of a terrorist event. Among the tested elements was the interaction of the EU Crisis Protocol with the new obligation for hosting service providers, introduced by article 14.5 of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, to promptly inform competent authorities when they become aware of terrorist content involving an imminent threat to life." READ MORE

Source: Bleeping Computer

Date: 01 March 2024

Germany takes down cybercrime market with over 180,000 users

"The Düsseldorf Police in Germany have seized Crimemarket, a massive German-speaking illicit trading platform with over 180,000 users, arresting six people, including one of its operators. Known as Crimemarket, it was the largest cybercrime market in the country and a hub for trading illegal drugs, narcotics, and cybercrime services, while it also hosted tutorials/guides for conducting various crimes." READ MORE

Source: La Tribune

Date: 11 March 2024

France : des attaques informatiques d'une « intensité inédite » frappent plusieurs services de l'Etat

"Plusieurs services de l'Etat ont été visés dimanche soir par des attaques informatiques d'une « intensité inédite », a indiqué ce lundi Matignon. Des attaques « inédites ». C'est ainsi que Matignon a qualifié les attaques informatiques qui ont touché plusieurs services de l'Etat depuis dimanche soir. Mais leur impact à ce stade « a été réduit » et l'accès aux sites de l'Etat « rétabli », a appris l'AFP lundi auprès de Matignon. Le ministère du Travail est notamment touché, selon une source interne au ministère. […] Ces attaques « ne sont pas attribuables aux Russes à ce stade », affirme cependant une source sécuritaire." READ MORE

RELATED ARTICLE:

Tech Monitor, French state cyberattack: Anonymous Sudan claims responsibility, 12 March 2024

Source: La Tribune

Date: 01 March 2024

L'État refuse de donner 41.000 euros pour sauver Point de Contact, maillon crucial dans la lutte contre la pédocriminalité en ligne

"C'est la somme qui manque à Point de Contact, l'un des acteurs les plus actifs en France dans la lutte contre les contenus illicites en ligne, pour poursuivre sa mission. Depuis 25 ans, cette petite équipe de six personnes épluche des dizaines de milliers de contenus signalés par les internautes, les catégorise, et les fait si besoin retirer du Web et remonter aux autorités." READ MORE

Source: The Royal Belgian Football Association (RBFA)

Date: 06 March 2024

Belgian Football Launches Campaign against Online Hate Speech

"The Royal Belgian Football Association (RBFA), the Pro League, ACFF and Voetbal Vlaanderen are fighting discrimination and racism in Belgian football with the Come Together action plan. However, hate speech does not stop on the sidelines, but increasingly continues online. This is why the Pro League and RBFA are launching several awareness-raising videos, in which Toby Alderweireld and Eleven DAZN face Séverine Parlakou, among others, share their stories." READ MORE

Source: US Attorney's Office

Date: 13 March 2024

United States Files Forfeiture Action to Recover Cryptocurrency Traceable to Pig Butchering Romance Scam

"[…] a Massachusetts resident was a victim of a romance scam and was tricked into wiring over $400,000 into a cryptocurrency wallet hosted by a legitimate cryptocurrency exchange. Some of those funds were subsequently transferred to other wallets and ultimately to Binance. Some of the funds were traced to two Binance accounts and the cryptocurrency was seized in January 2024. The investigation revealed that the accounts from which the cryptocurrency was seized had been associated with funds from 36 other victims of fraud located across the United States. It is a violation of federal law to use wire communications as part of a scheme to defraud or to obtain money or property by means of false or fraudulent pretenses." READ MORE

Source: Security Affairs

Date: 09 March 2024

Threat actors hacked the systems of the Cybersecurity and Infrastructure Security Agency (CISA) by exploiting Ivanti flaws.

"The US Cybersecurity and Infrastructure Security Agency (CISA) agency was hacked in February, the Recorded Future News first reported. In response to the security breach, the agency had to shut down two crucial systems, as reported by a CISA spokesperson and US officials with knowledge of the incident, according to CNN. One of the systems impacted by the incident is used to facilitate the sharing of cyber and physical security assessment tools among federal, state, and local officials. The second system was holding information related to the security assessment of chemical facilities." READ MORE

Source: ABC News

Date: 13 March 2024

Sunshine Coast man Dion Adam Lingard charged with 116 child abuse offences

"Dion Adam Lingard, 31, has been charged with 116 offences, including rape, indecent treatment of a child, stalking, and making child exploitation material allegedly involving two young girls in the North Coast region. […] Police said they started the investigation after they allegedly discovered Mr Lingard was targeting children online who he did not know. […] Detective Inspector Toohey said parents needed to be vigilant how their children used internet-connected devices. "We're inviting offenders into their bedrooms if we allow children to take their devices there," he said." READ MORE

Source: GMA Network

Date: 14 March 2024

DOJ launches guidelines in case build-up of online, gender-based sexual harassment

"The Department of Justice (DOJ) on Thursday announced that it has launched guidelines in the gathering of evidence and case build-up of gender-based online sexual harassment (GBOSH). According to the DOJ, the move is in collaboration with the Philippine National Police (PNP) and the National Bureau of Investigation (NBI) in order to establish clear procedures for receiving complaints, addressing incidents and collecting evidence." READ MORE

Source: The Record

Date: 05 March 2024

Cyberattack forces Canada's financial intelligence agency to take systems offline

"The agency is the national authority for suspicious transactions, including those relating to terrorist financing, and a partner to the country's intelligence and law enforcement agencies. […] The nature of the incident has not been disclosed, and so it is not possible to infer whether the attack was financially motivated or perpetrated by attackers seeking access to FINTRAC intelligence — although the agency said it "does not involve the Centre's intelligence or classified systems." READ MORE

Source: Cybernews

Date: 04 March 2024

Canada Supreme Court: no search warrant, no IP

"From now on, Canadian police will need to obtain a search warrant to access an IP address, a landmark ruling by the Supreme Court has determined. The case was brought by convicted cybercriminal Andrei Bykovets, who was found guilty of 14 cases of online fraud after police tracked him down using IP addresses obtained from the website where he made the illicit purchases using stolen credit card details. […] The fresh ruling sets a landmark precedent under Canadian law, determining that if the law's purpose "is to meaningfully protect the online privacy of Canadians in today's overwhelmingly digital world, it must protect their IP addresses." READ MORE

Latest reports

- Clingendael, Too late to act? Europe's quest for cloud sovereignty, 01 March 2024
- Sucuri Blog, New Wave of SocGholish Infections Impersonates WordPress Plugins, 01 March 2024
- Eset, Tendências de cibersegurança para 2024 antecipam aumento de ataques e impacto significativo da inteligência artificial no cibercrime, 01 March 2024
- Bleeping Computer, Stealthy GTPDOOR Linux malware targets mobile operator networks, 03 March 2024
- Trend Micro, Multistage RA World Ransomware Uses Anti-AV Tactics, Exploits GPO, 04 March 2024
- Africa Cybersecurity Magazine, Attaques par ransomware, Afrique du Sud : huitième au monde, 04 March 2024
- Asia Times, Bytes to battles: a short cyberwar history, 04 March 2024
- Radio France, Le hameçonnage, principale menace numérique, selon un rapport de la plateforme Cybermalveillance, 05 March 2024
- ONU, Industrie du divertissement : abus sexuels et exploitation des enfants sont très répandus, selon une experte, 05 March 2024
- SecureList, Network tunneling with… QEMU?, 05 March 2024
- Talos Intelligence, GhostSec's joint ransomware operation and evolution of their arsenal, 05 March 2024
- Dark Reading, Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure, 05 March 2024
- Cyber Security News, Project DDoSia – Russian Hackers "NoName057(16)" Planning Massive DDoS Attack, 05 March 2024
- Ukrainska Pravda, Large numbers of Russian university students being taught hacking – Ukraine's Security Service, 05 March 2024
- European Commission, New Cybersecurity compendium on how to protect integrity of elections published, 06 March 2024
- Oxford University Press, Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty, 06 March 2024
- Digital Inside, A IA ao serviço do cibercrime, 06 March 2024
- Cyble, SapphireStealer Sneaks In: Deceptive Legal Documents Prey on Russians, 06 March 2024
- Symantec Security, Data Exfiltration: Increasing Number of Tools Leveraged by Ransomware Attackers, 06 March 2024
- FBI, Internet Crime Report 2023, 06 March 2024
- Cado Security, Spinning YARN - A New Linux Malware Campaign Targets Docker, Apache Hadoop, Redis and Confluence, 06 March 2024
- Proof Point, TA4903: Actor Spoofs U.S. Government, Small Businesses in Phishing, BEC Bids, 06 March 2024
- Council of Europe, Council of Europe takes stock of the work to protect children's rights since 2022, 06 March 2024
- AttackIQ, Response to the Revised CISA Advisory (AA23-353A): #StopRansomware: ALPHV BlackCat, 07 March 2024

- Black Berry, The AI Standoff: Attackers vs. Defenders, 07 March 2024
- LWYR, La violencia de género en espacios digitales y su actual regulación, 07 March 2024
- Guidepoint Security, BianLian GOs for PowerShell After TeamCity Exploitation, 08 March 2024
- INTERPOL, INTERPOL Financial Fraud assessment: A global threat boosted by technology, 11 March 2024
- The Cyber Express, Cyber Infiltration and Influence: Baltic States in Russia's Crosshairs, 11 March 2024
- Radio Canada, Les cas déclarés d'exploitation sexuelle en ligne de mineurs en hausse au Canada, 12 March 2024
- Cyble, Xehook Stealer: Evolution of Cinoshi's Project Targeting Over 100 Cryptocurrencies and 2FA Extensions, 12 March 2024
- Sophos News, The 2024 Sophos Threat Report: Cybercrime on Main Street, 12 March 2024
- SecureList, Top 10 web application vulnerabilities in 2021–2023, 12 March 2024
- Fortinet, VCURMS: A Simple and Functional Weapon, 12 March 2024
- Reversing Lab Blogs, BIPClip: Malicious PyPI packages target crypto wallet recovery passwords, 12 March 2024
- Infosecurity magazine, New Cloud Attack Targets Crypto CDN Meson Ahead of Launch, 12 March 2024
- Kaspersky, Global Kaspersky report reveals digital violence has increased, 13 March 2024
- Securelist, The State of Stalkerware in 2023–2024, 13 March 2024
- Akamai, What a Cluster: Local Volumes Vulnerability in Kubernetes, 13 March 2024
- Talos Intelligence, Threat actors leverage document publishing sites for ongoing credential and session token theft, 13 March 2024
- Salt Security, Security Flaws within ChatGPT Ecosystem Allowed Access to Accounts On Third-Party Websites and Sensitive Data, 13 March 2024
- SecurityWeek, Major CPU, Software Vendors Impacted by New GhostRace Attack, 13 March 2024
- BlackBerry, Systems Under Siege: BlackBerry Report Reveals Millions of Attacks Targeting Critical Infrastructure, 14 March 2024
- SecureList, A patched Windows attack surface is still exploitable, 14 March 2024
- The Guardian, Violent online content 'unavoidable' for UK children, Ofcom finds, 15 March 2024
- Article 19, UN: Cybercrime Convention still deeply flawed after seven sessions, 15 March 2024

Upcoming events

- 18 March 2024, C-PROC, (online), Meeting with Momentum project team (INTERPOL) to discuss joint activities, CyberSouth+
- 19 March 2024, C-PROC, (online), Meeting with the European Cybercrime Training and Education Group (ECTEG) team to discuss their courses and possible collaboration for implementation of activities, CyberSouth+
- 20 March 2024, C-PROC, (online), Co-ordination meeting with the Palestinian authorities to discuss co-operation under CyberSouth+
- 20 March 2024, C-PROC, (online), Co-ordination meeting with the Lebanese representatives to discuss regional activities, CyberSouth+
- 26 March 2024, C-PROC, (online), Meeting with the Libyan institutions to discuss future co-operation under CyberSouth+
- 26 March 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
- 27 March 2024, C-PROC, (in person), Meeting with the representatives of the Italian Embassy in Romania to present the new project, CyberSouth+
- 26-28 March 2024, Forum InCyber Europe (in person), Lille, France, T-CY
- 28-30 March 2024, C-PROC/MAURITIUS, (in person), Training of Trainers: Introductory Judicial Training on cybercrime and electronic evidence (magistrates and prosecutors), GLACY-e
- March 2024, C-PROC (online), Monitoring and analysis for the online resource on cyberviolence, Octopus
- March 2024, C-PROC, (online), Further development of the Octopus Platform, Octopus
- March 2024, C-PROC, (online), Further development of the CYBOX training platform, Octopus
- March, C-PROC/ECUADOR, (online), Development of a specialised module on gendered aspects of cybercrime in Ecuador, GLACY-e
- March-May 2024, C-PROC, (online), ASEAN regional study on legislation, Octopus
- March-June 2024, T-CY (online), Continued assessment of the implementation by Parties of the Art. 19 of the Convention on Cybercrime, T-CY

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