Cybercrime Digest

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

1 - 15 January 2024

Source: Council of Europe

Date: 03 January 2024

75th anniversary year for the Council of Europe

"2024 will mark the 75th anniversary of the Council of Europe - an occasion to raise awareness of the Organisation's positive impact on people's daily lives over three-quarters of a century, protecting human rights, democracy, and the rule of law. It will also be an opportunity to look forward and highlight the work that our member states are undertaking to promote and implement our shared values and standards." READ MORE

Source: European Commission

Date: 11 January 2024

European Data Act enters into force, putting in place new rules for a fair and innovative data economy

"The new rules define the rights to access and use data generated in the EU across all economic sectors and will make it easier to share data, in particular industrial data. The Data Act will ensure fairness in the digital environment by clarifying who can create value from data and under which conditions. It will also stimulate a competitive and innovative data market by unlocking industrial data, and by providing legal clarity as regards the use of data." READ MORE

Source: US Department of Justice

Date: 04 January 2024

19 Individuals worldwide charged in transnational cybercrime investigation of the xDedic marketplace

"United States Attorney Roger B. Handberg announces the culmination of a transnational cybercrime investigation involving the xDedic Marketplace. According to court documents, the xDedic Marketplace was a website on the dark web that illegally sold login credentials (usernames and passwords) to servers located across the world and personally identifiable information—dates of birth and Social Security numbers—of U.S. residents. Once purchased, criminals used these servers to facilitate a wide range of illegal activity that included tax fraud and ransomware attacks." READ MORE

Source: European Commission

Date: 09 January 2023

Commission launches calls for contributions on competition in virtual worlds and generative AI

"The European Commission has launched today two calls for contributions on competition in virtual worlds and generative artificial intelligence ('AI') and sent requests for information to several large digital players. All interested stakeholders are invited to share their experience and provide feedback on the level of competition in the context of virtual worlds and generative AI, and their insights on how competition law can help ensure that these new markets remain competitive. The European Commission will carefully review all input received through the calls for contributions." READ MORE

Source: ASPI

Date: 15 January 2024

Building trust in artificial intelligence: lessons from the EU AI Act

"Artificial intelligence will radically transform our societies and economies in the next few years. The world's democracies, together, have a duty to minimise the risks this new technology poses through smart regulation, without standing in the way of the many benefits it will bring to people's lives. There is strong momentum for AI regulation in Australia, following its adoption of a government strategy and a national set of AI ethics. Just as Australia begins to define its regulatory approach, the European Union has reached political agreement on the EU AI Act, the world's first and most comprehensive legal framework on AI. That provides Australia with an opportunity to reap the benefits from the EU's experiences." READ MORE

Source: Europol

Date: 12 January 2024

Cryptojacker arrested in Ukraine over EUR 1.8 million mining scheme

"The National Police of Ukraine (Національна поліція України), with the support of Europol, has arrested an individual believed to be the mastermind behind a sophisticated cryptojacking scheme. The 29-year-old individual was apprehended in Mykolaiv, Ukraine, on 9 January. Three properties were searched to gather evidence against the main suspect. The arrest comes after months of intensive collaboration between Ukrainian authorities, Europol and a cloud provider, who worked tirelessly to identify and locate the individual behind the widespread cryptojacking operation." READ MORE

Source: World Economic Forum

Date: 10 January 2024

2023 was a big year for cybercrime – here's how we can make our systems safer

"Our definition of what a criminal is, is changing. Where in the past, you might have thought of a shady character trying to breach the boundaries of your home and steal your possessions, those who commit crimes in this decade are far less easy to conjure up in your mind – faceless, formless and more likely to hide behind a computer. Cybercrime is a real and growing threat, with the global cost of online criminal acts expected to surge to $23.84 trillion by 2027, up from $8.44 trillion in 2022, according to data from Statista, the FBI and IMF." READ MORE

Source: Reuters

Date: 05 January 2024

Russian hackers were inside Ukraine telecoms giant for months

"Russian hackers were inside Ukrainian telecoms giant Kyivstar's system from at least May last year in a cyberattack that should serve as a "big warning" to the West, Ukraine's cyber spy chief told Reuters. The hack, one of the most dramatic since Russia's full-scale invasion nearly two years ago, knocked out services provided by Ukraine's biggest telecoms operator for some 24 million users for days from Dec. 12. In an interview, Illia Vitiuk, head of the Security Service of Ukraine's (SBU) cybersecurity department, disclosed exclusive details about the hack, which he said caused "disastrous" destruction and aimed to land a psychological blow and gather intelligence." READ MORE

Source: Association for progressive communications

Date: 08 January 2024

From buttocks to electronic bracelets: How governments are using cybercrime laws to target women and LGBTQIA+ people

"In 2021, 34-year-old PhD student Salma al-Shehab was sentenced by Saudi Arabia to 34 years in prison and 34 years of travel restrictions for a cybercrime. In 2022, 73-year-old Olga Mata was confronted with a potential sentence of 10 to 20 years for what the Venezuelan government deemed a hate crime online. In 2023, 19-year-old Russian student Olesya Krivtsova was charged with the crime of "fake news" and "acts justifying terrorism" – charges that could mean a 10-year prison term." READ MORE

Source: Humanitarian Law & Policy

Date: 04 January 2024

Online violence: real life impacts on women and girls in humanitarian settings

"Online violence is not contained by the digital sphere – it is killing women and adolescent girls in offline spaces. It seeps into their daily lives, infecting their psychological and physical well-being and resulting in paranoia, shame, isolation, and even leading to their deaths through honor killing, murder, and suicide." READ MORE

Source: International Bar Association

Date: 09 January 2024

Digital Services Act & Digital Markets Act: Europe regulates big digital platforms – perspectives in Argentina, Brazil, and the United States

"With the premise that 'what is illegal in the real world must be illegal online' the EU, together with the European Commission, the European Parliament and the European Council, started discussing, during 2020, two projects that aim to regulate digital platforms: the Digital Services Act (DSA) and the Digital Markets Act (DMA). Both Acts, which formed part of the regulatory package known as the 'Digital Services Package', came into force in November 2022 and are already projecting effects in the daily operation of digital platforms in the EU." READ MORE

Source: Coin Telegraph

Date: 11 January 2024

Binance amplía colaboración en ciberseguridad con INTERPOL en Latam

"Binance anunció colaboración y participación en talleres organizados por INTERPOL, el Ministerio Público de Chile, el Consejo de Europa, así como la Policía Nacional de Colombia. Pablo Vera, jefe de Inteligencia e Investigaciones de Binance en las Américas, participó en una conferencia de INTERPOL en la República Dominicana, con más de 50 directivos y líderes de unidades policiales especializadas en ciberseguridad. En esa ocasión, realizó una presentación individual y participó en un panel sobre criptomonedas, apoyo a las fuerzas del orden, cumplimiento e investigaciones." READ MORE

Source: Eurojust

Date: 12 January 2024

Eurojust and Panama sign Working Arrangement to step up cooperation against organised crime

"Eurojust and the Attorney General of the Republic of Panama, Mr Javier E. Caraballo Salazar, have signed a Working Arrangement today to enable structured and closer cooperation in the fight against organised crime. The agreement formalises Eurojust's existing Contact Points in Panama and ensures closer communication to speed up the execution of judicial cooperation requests on both sides. Panama is the first Latin American country to sign a Working Arrangement with the Agency." READ MORE

Source: Centro Nacional de Ciberseguridad

Date: 12 January 2024

Dominican Republic: Gobierno lanza servicio de alerta automática ante vulnerabilidades y exposición en el ciberespacio

"El Gobierno, a través del Centro Nacional de Ciberseguridad (CNCS), puso a disposición de las entidades públicas y privadas un servicio de notificación automática de vulnerabilidades y exposición en el ciberespacio. El nuevo servicio, que se ofrece de forma gratuita, tiene por finalidad ayudar a las organizaciones a fortalecer su ciberseguridad y proteger sus activos digitales para impulsar un ciberespacio más seguro, confiable y resiliente, a través de las notificaciones oportunas. El recurso, presentado por el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), junto a la Fundación Shadowserver, está alineado a la Agenda Digital 2030, nuestra Estrategia Nacional de Transformación Digital." READ MORE

Source: The Guardian

Date: 11 January 2024

Visitors to Colombia warned over dating apps after eight US deaths in two months

"Foreign visitors to Colombia should take serious caution when using dating apps after a spate of suspicious deaths in the South American country, the US embassy in Bogotá has warned. In the last two months of 2023, eight US citizens died in the city of Medellín, in incidents involving drugging or suspected murder. Several of the cases were linked to dating apps, according to a state department security alert on Wednesday." READ MORE

Source: Cyber Security Intelligence

Date: 22 December 2023

Enormous leak - Brazil's population data exposed

"The leaked data, which has not been linked to a specific company or organisation so far, contained more than 223 million records, which implies that the entire Brazilian population might be affected by the leak. While the data is no longer publicly available, in the hands of a malicious actor, the exposed data could have been misused for identity theft, fraud, and targeted cybercrimes. This could result in financial losses, unauthorised access to personal accounts, and other severe consequences for those individuals whose personal data was exposed." READ MORE

Source: Global Economic Governance Programme

Date: January 2024

Nnenna Ifeanyi-Ajufo : « L'état actuel de la cybersécurité en Afrique est la tendance à la cyber-militarisation de la cybergouvernance »

" […] L'Afrique reste la région la plus faible en termes de digitalisation, ce qui a un impact sur son approche de la cybersécurité. La disparité dans la répartition des richesses entre les pays africains joue un rôle important dans ce contexte. Dans les pays les plus pauvres, la cybersécurité n'est souvent pas une priorité, et dans des régions comme le Sahel, les conflits et l'instabilité politique nuisent encore plus aux initiatives en matière de cybersécurité." READ MORE

Source: L'Opinion

Date: 09 January 2024

Morocco: Parlement: Les solutions de Ouahbi pour le système judiciaire marocain

"Interrogé sur la montée en puissance de la cyber-violence faite aux femmes, le ministre de la Justice a reconnu le vide juridique persistant, l'attribuant à l'absence de plaintes. Le ministre a affirmé dans ce sens "qu'une bonne partie des femmes victimes de ces actes criminels choisissent de les endurer en silence au lieu de porter plainte". Rappelons à ce titre que l'enquête nationale sur la prévalence de la violence à l'égard des femmes, réalisée par le Haut-Commissariat au Plan (HCP), a montré que la cyber-violence touche près d'1,5 million de femmes (13,8%) au Maroc." READ MORE

Source: Hack Read

Date: 08 January 2024

Lebanon: Beirut airport screens hacked with anti-Hezbollah message

"The information display screens at Beirut's international airport were hacked by anti-Hezbollah groups, highlighting the intensification of ongoing clashes between the Lebanese militant group and the Israeli military. The screens, which display arrival/departure times, displayed a message accusing Hezbollah of putting Lebanon at risk of war with Israel. "Hassan Nasrallah, you will no longer have supporters if you curse Lebanon with a war for which you will bear responsibility and consequences," the message read." READ MORE

Source: Human Rights Watch

Date: 11 January 2024

Jordan: New threats to civic space

"Jordanian authorities in 2023 limited civic space and enacted a new cybercrime law that further undermines free speech and privacy online, Human Rights Watch said today in its World Report 2024. Jordanian authorities arrested and harassed peaceful dissidents and journalists and used vague and abusive laws to limit free speech and peaceful activism." READ MORE

Source: The Record

Date: 08 January 2024

Bangladesh official alleges cyberattack 'from Ukraine and Germany' targeted election

"An official at the Bangladesh Election Commission has claimed that a cyberattack "from Ukraine and Germany" caused an election information app to crash as voters went to the polls on Sunday. There has not been an allegation that the incident affected votes in the country, […]." READ MORE

Source: Pakistan Today

Date: 11 January 2024

Pakistan: First cybercrime investigation unit established in capital to combat digital offences

"The Islamabad Police to vigorously combat the cybercrimes has made the newly inaugurated Cyber Crime Investigation Unit as its part. The initiative was taken after amendments to the Prevention of Electronic Crimes Act (PECA), empowering Islamabad Police to register cybercrime cases under Section 30. Seeking to harness specialized expertise, Islamabad Police have collaborated with the Federal Investigation Agency (FIA) to leverage technical assistance in the investigation of cybercrimes." READ MORE

Source: India TV news

Date: 05 January 2024

India: G20 Summit website faced persistent cyberattacks last year, 16 lakh attempts detected per minute: Centre

"The Indian cybersecurity sector successfully thwarted numerous cyberattack attempts on the G20 portal during the summit, with a peak of 16 lakh Distributed Denial of Service (DDoS) attacks per minute. Rajesh Kumar, the CEO of the Indian Cybercrime Coordination Centre (I4C), disclosed this information at the annual conference." READ MORE

Source: The Week

Date: 10 January 2024

Maldives government website down after suspected cyber-attack; hackers claim to be Indians

"Two days after hackers targeted the official websites of the Maldivian President's Office, Foreign Ministry and Tourism Ministry, the web platform of the Juvenile Court of the Maldives too has apparently come under cyber-attack on Wednesday. The website, which is no longer available, earlier showed a message from a group of hackers TeaM NETWORK9, claiming to be Indians." READ MORE

Source: GovInsider

Date: 10 January 2024

South Korea's 56 hours of paralysis is a cyber resilience cautionary tale

"A series of outages of unprecedented scale rocked the East Asian country's digital government network, hampering civil servants and inconveniencing citizens, who filed 240,000 complaints. GovInsider looks at the lessons learned about cyber security and resilience." READ MORE

Source: The Hacker News

Date: 08 January 2024

North Korea's Cyber Heist: DPRK Hackers Stole $600 Million in Cryptocurrency in 2023

"Threat actors affiliated with the Democratic People's Republic of Korea (also known as North Korea) have plundered at least $600 million in cryptocurrency in 2023. The DPRK "was responsible for almost a third of all funds stolen in crypto attacks last year, despite a 30% reduction from the USD 850 million haul in 2022," blockchain analytics firm TRM Labs said last week." READ MORE

Source: The Japan Times

Date: 03 January 2023

Misinformation on Japan quake spreading on social media, government warns

"False information concerning a powerful earthquake in central Japan on New Year's Day has been spreading on social media platforms, prompting the government on Wednesday to call for the public to exercise caution. Some posts have attributed the cause of the magnitude 7.6 quake that struck the Noto Peninsula and its vicinity on the Sea of Japan coast on Monday to the use of an "earthquake weapon," while describing the seismic event as an "artificial earthquake."" READ MORE

Source: The Straits Times

Date: 08 January 2024

New $20m project by British and Singapore researchers to improve healthcare cyber security

"Hackers targeting life-saving healthcare devices like pacemakers is not just science fiction, but could become reality in the not-so-distant future as medical devices become more connected. To prepare for such scenarios and more, scientists from Imperial College London and Nanyang Technological University (NTU) will embark on a $20 million programme to improve the cyber security of medical devices." READ MORE

Source: VOA News

Date: 23 December 2023

Cyberbullying hinders women's participation in Indonesia's 2024 elections

"Online bullying of women and girls in Indonesia skyrocketed during the COVID-19 pandemic, and this disturbing trend has continued and even intensified ahead of the February 14, 2024 elections. Cyberbullying makes women more reluctant to participate online which exacerbates the gender digital divide." READ MORE

Source: Manila Bulletin

Date: 05 January 2024

Philippines: Cybercrime: You could be the next victim

"The incidence of cybercrime has been rising around the world, especially in developing countries where many remain unfamiliar with the internet and the risks it presents. […] One of the private sector's initiative, #ScamWatchPH, co-founded by Manila Bulletin (MB) and reputation management brand Truth360, is a cybersecurity movement that aims to educate Filipinos on how to protect themselves against cyber fraud and online scams." READ MORE

Source: Papa New Guinea Today

Date: 09 January 2024

PNG ICT Minister Timothy Masiu Reflects on Pivotal Year, Charts Vision for 2024

"In his New Year's address, the Papua New Guinea (PNG) Minister for Information and Communication Technology (ICT), Timothy Masiu, offered reflections on a momentous year for Papua New Guinea's ICT sector and outlined a visionary roadmap for the upcoming year." READ MORE

Source: cyberdaily.au

Date: 15 January 2024

Australia: Home Affairs unable to say who was responsible for October cyber attack

"A spokesperson for the Department of Home Affairs has told Senate estimates that, despite a lengthy investigation, it has been unable to determine who was behind a cyber attack that took its website offline last October. "As with most DDoS attacks, the threat actor disguised their activities through the use of multiple IP addresses, making the attribution of the origin difficult, if not impossible," Home Affairs said in response to a question on notice, as reported by The Guardian. […] However, despite the Home Affairs investigation not turning up a culprit, the pro-Russian hacktivist group Noname057(16) took responsibility for the hack at the time. The group boasted on its Telegram channel on 5 October 2023 that it was responsible for taking down the government site." READ MORE

Source: it news

Date: 15 January 2024

Australia: Commonwealth DPP taking briefs on deepfakes from police

"The Commonwealth Director of Public Prosecutions (CDPP) is already handling evidentiary briefs involving the use of deepfakes but is worried at its ability to act on them. Deepfakes are typically images that are manipulated using artificial intelligence to depict things that never happened. The prosecution service is concerned at the limited options under the federal criminal code to pursue a case involving deepfakes, and - as a result - at the maximum possible sentence that can be imposed." READ MORE

Source: The Astana Times

Date: 15 January 2024

Kazakhstan registers significant attempts of cyber-attacks in 2023

"Kazakhstan registered more than 223 million attempted cyber-attacks carried out by foreign hackers in 2023, according to the State Technical Service. The highest number of cyber-attacks, nearly 133.5 million, attempted to undermine local executive bodies. Government agencies were hit by some 47.7 million cyber-attacks, and the quasi-public sector suffered around 27 million attempted hacks. Telecom operators had some 19.9 million cyber-attack attempts, and private companies reported 2.9 million hacks." READ MORE

Source: Yahoo News

Date: 08 January 2024

Ukrainian soldiers are sent malware disguised as information on recruitment to 3rd Separate Assault Brigade and IDF

"Hackers have been sending soldiers of the Armed Forces of Ukraine (AFU) messages containing malware that purports to concern recruitment to the 3rd Separate Assault Brigade and Israel Defence Forces (IDF)." READ MORE

RELATED ARTICLE:

CERT-UA, UAC-0184: Цільові атаки у відношенні українських військовослужбовців з використанням тематики рекрутингу до 3 ОШБр та ЦАХАЛ (CERT-UA#8386), 6 January 2024

Source: The Cyber Express

Date: 08 January 2024

NoName on Rampage! Claims DDoS Attacks on Ukrainian Government Sites

"NoName ransomware group has allegedly targeted multiple Ukrainian government websites. The latest victims of the alleged NoName ransomware attack on Ukraine include Accordbank, Zaporizhzhya Titanium-Magnesium Plant, State Tax Service, Central Interregional Tax Administration, Western Interregional Tax Administration, and the Main Directorate of the State Tax Service in Kyiv. The Cyber Express tried to verify the claims made by the threat actor and found the website of Zaporizhzhya Titanium-Magnesium Plant operational at the moment." READ MORE

Source: Reuters

Date: 09 January 2024

Hackers hit Moscow internet provider in response to Kyivstar cyber-attack - source

"Hackers linked to Ukraine's main spy agency have breached computer systems at a Moscow-based internet provider in retaliation for a Russian cyber-attack against Ukrainian telecom giant Kyivstar, a source with direct knowledge of the operation told Reuters on Tuesday. The hacking group, dubbed "Blackjack", has previously been linked to the Security Service of Ukraine (SBU). The hackers deleted 20 terrabytes of data at M9 Telecom, a small Russian internet and TV provider, leaving some Moscow residents without internet, the source said." READ MORE

Source: Covington

Date: 14 January 2024

EU Supervisory Authorities publish new guidance on cookies

"Several EU data protection supervisory authorities ("SAs") have recently issued guidance on cookies. On January 11, 2024, the Spanish SA published guidance on cookies used for audience measurement (often referred to as analytics cookies) (available in Spanish only). On December 20, 2023, the Austrian SA published FAQs on cookies and data protection (available in German only). On October 23, 2023, the Belgian SA published a cookie checklist (available in Dutch and French)." READ MORE

Source: The Hacker News

Date: 06 January 2024

Sea Turtle cyber espionage campaign targets Dutch IT and telecom companies

"Telecommunication, media, internet service providers (ISPs), information technology (IT)-service providers, and Kurdish websites in the Netherlands have been targeted as part of a new cyber espionage campaign undertaken by a Türkiye-nexus threat actor known as Sea Turtle. "The infrastructure of the targets was susceptible to supply chain and island-hopping attacks, which the attack group used to collect politically motivated information such as personal information on minority groups and potential political dissents," Dutch security firm Hunt & Hackett said in a Friday analysis. […] Activities associated with the group are believed to have been ongoing since January 2017, primarily leveraging DNS hijacking to redirect prospective targets attempting to query a specific domain to an actor-controlled server capable of harvesting their credentials." READ MORE

Source: CNIL

Date: 11 January 2024

Paiement électronique: la CNIL inflige une amende de 105 000 euros à NS CARDS FRANCE

"Le 29 décembre 2023, la CNIL a prononcé une sanction de 105 000 euros à l'encontre de la société NS CARDS FRANCE pour le non-respect des règles sur les cookies et traceurs ainsi que pour plusieurs manquements au RGPD, concernant la durée de conservation des données, l'information des personnes et la sécurité des données." READ MORE

RELATED ARTICLE:

EDPB, Commercial prospecting and personal rights: French SA fined NS CARDS FRANCE €105,000, 15 January 2024

Source: Swiss Info

Date: 06 January 2024

Cyberattack exposes Swiss Air Force documents on the darknet

"The Swiss Air Force has been victim to a malicious cyber attack. The group allegedly responsible for the data breach is suspected to originate from Russia. A US security company, providing communication technology to defence firms globally, fell victim to a cyberattack. The Swiss Air Force was among the entities affected. Switzerland's Federal Department of Defence has officially confirmed the data breach and is currently investigating the incident." READ MORE

Source: Security Affairs

Date: 04 January 2024

Hacker hijacked Orange Spain ripe account causing internet outage to company customers

"An internet outage impacted Orange Spain after a hacker gained access to the company's RIPE account to misconfigure BGP routing. The hacker, who uses the moniker 'Snow', gained access to the RIPE account of Orange Spain and misconfigured the BGP routing causing an internet outage. The customers of the company were not able to access the internet for several hours on January 3 as a result of the attack." READ MORE

Source: Bleeping Computer

Date: 11 January 2024

Finland warns of Akira ransomware wiping NAS and tape backup devices

"The Finish National Cybersecurity Center (NCSC-FI) is informing of increased Akira ransomware activity in December, targeting companies in the country and wiping backups. The agency says that the threat actor's attacks accounted for six out of the seven cases of ransomware incidents reported last month." READ MORE

Source: The Guardian

Date: 10 January 2024

UK: Children now 'biggest perpetrators of sexual abuse against children'

"Boys are watching violent porn on their smartphones then going on to attack girls, police have said, as new data showed children are now the biggest perpetrators of sexual abuse against other children. Police data shows there has been a quadrupling of sexual offences against children, in what officers say is the most authoritative analysis of offending against youngsters." READ MORE

Source: Internet Watch Foundation

Date: 11 January 2024

UK: Don't delay talking to girls about keeping safe online, parents urged

"Research from Anglia Ruskin University's Policing Institute for the Eastern Region (PIER) shows that two-way communication, as well as careful monitoring, is the most effective way to prepare girls to handle online requests for indecent images. The research draws on survey results that were conducted following a public awareness campaign run by the Internet Watch Foundation (IWF) in 2021. The UK charity is responsible for finding and removing images and videos of child sexual abuse from the internet. The campaign aimed to build resilience among girls, and their parents, around online requests for sexual imagery." READ MORE

Source: National Institute of Standards and Technology

Date: 04 January 2024

US: NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

"Adversaries can deliberately confuse or even "poison" artificial intelligence (AI) systems to make them malfunction — and there's no foolproof defense that their developers can employ. Computer scientists from the National Institute of Standards and Technology (NIST) and their collaborators identify these and other vulnerabilities of AI and machine learning (ML) in a new publication. Their work, titled Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (NIST.AI.100-2), is part of NIST's broader effort to support the development of trustworthy AI, and it can help put NIST's AI Risk Management Framework into practice." READ MORE

Source: Reuters

Date: 11 January 2024

US SEC approves bitcoin ETFs in watershed for crypto market

"The U.S. securities regulator on Wednesday approved the first U.S.-listed exchange traded funds (ETFs) to track bitcoin, in a watershed for the world's largest cryptocurrency and the broader crypto industry. The Securities and Exchange Commission said it approved 11 applications, including from BlackRock (BLK.N), Ark Investments/21Shares (ABTC.S), Fidelity, Invesco (IVZ.N) and VanEck, despite warnings from some officials and investor advocates that the products carried risks." READ MORE

RELATED ARTICLE:

Reuters, Why a US bitcoin ETF is a game-changer for crypto, 11 January 2024

Source: IT World Canada

Date: 11 January 2024

Canadian Cyber Centre now ranks threats with SecurityScorecard solution

"The Canadian government's cyber authority has started using a U.S. company's security ratings platform to rank cyber threats to the country's critical infrastructure. The Canadian Centre for Cyber Security said Thursday it has contracted to use SecurityScorecard's security ratings platform. Under an arrangement with the company, the scoring will help the Cyber Centre educate critical infrastructure owner-operators on the risks facing their organizations, assisting them in remediating and measuring cybersecurity risks." READ MORE

Latest reports

- The Hacker News, New variant of DLL search order hijacking bypasses Windows 10 and 11 Protections, 1 January 2024
- Twenty four, UK Cybercrime Statistics 2024, 2 January 2024
- Netmission.asia, Asia Pacific Policy Observatory Report – December 2023: A Fight for Online Safety and Digital Rights: An Overview of Recent Policy Developments in Australia, Nepal, and Myanmar, 2 January 2024
- CISA, CISA adds two known exploited vulnerabilities to catalog, 2 January 2024
- Security Affairs, Cybercriminals implemented Artificial Intelligence (AI) for invoice fraud, 3 January 2024
- Trip Wire, Is Cybercrime Only Going to Get Worse?, 3 January 2024
- CYFIRMA, A gamer turned malware developer: diving into silverrat and it's Syrian roots, 3 January 2024
- The Hacker News, SMTP Smuggling: New Flaw Lets Attackers Bypass Security and Spoof Emails, 3 January 2024
- Searchlight Cyber, 2023 in review: threat actors and motivations, 3 January 2024
- ASEC, Internal Reconnaissance in Domain Environments Detected by EDR, 3 January 2024
- Signaturit, Electronic evidence and its admissibility in court, 4 January 2024
- The CTO club, 12 Best Digital forensics software shortlist, 4 January 2024
- Embroker, 2024 Must-know cyber-attack statistics and trends, 4 January 2024
- It Governance, List of data breaches and cyber-attacks in 2023 – 8,214,886,660 records breached, 5 January 2024
- Deseret News, Artificial intelligence will likely impact cyber kidnappings. Here's what you need to know, 5 January 2024
- AT&T Business, AsyncRAT loader: Obfuscation, DGAs, decoys and Govno, 5 January 2024
- SentinelOne, Unseen threats in software development | The perils of Trojanized NPM packages, 8 January 2024
- MSSP Alert, Top 10 Cyberattacks of 2023, 8 January 2024
- Check Point Research, .NET hooking – harmonizing managed territory, 8 January 2024
- Europol, Europol cybercrime training competency framework, 9 January 2024
- Bitdefender, 2024 Cybersecurity Predictions for AI: A Technical Deep Dive, 9 January 2024
- Recorded Future, 2023 Adversary infrastructure report, 9 January 2024
- Reuters Institute, Journalism, media, and technology trends and predictions 2024, 9 January 2024
- Trend Micro, Black Basta-Affiliated Water Curupira's Pikabot Spam Campaign, 9 January 2024
- World Economic Forum, Global Risks Report 2024: The risks are growing — but so is our capacity to respond, 10 January 2024
- Infosecurity-magazine, Only 4% of US States fully prepared for cyber-attacks targeting elections, 10 January 2024
- AT&T Business, Social engineering attacks: Real-life examples and how to avoid them, 10 January 2024

- Malwarebytes LABS, Atomic Stealer rings in the new year with updated version, 10 January 2024
- Akamai, You had me at hi — Mirai-Based NoaBot makes an appearance, 10 January 2024
- CompariTech, 300+ Terrifying cybercrime and cybersecurity statistics (2024 EDITION), 11 January 2024
- Chainalysis, CSAM and cryptocurrency: On-chain analysis suggests CSAM vendors may benefit from privacy coins like Monero and other obfuscation measures, 11 January 2024
- Help Net Security, Critical Cisco Unity Connection flaw gives attackers root privileges. Patch now! (CVE-2024-20272), 11 January 2024
- The Hacker News, New PoC exploit for Apache OfBiz vulnerability poses risk to ERP systems, 11 January 2024
- Tribune, Cyber incidents hit 15% of global firms, 11 January 2024
- Security Week, Researchers flag FBot hacking tool hijacking cloud, payment services, 11 January 2024
- Cyber News, India's Cherrinet ISP leaks user data, exposes accounts to abuse attempts, 11 January 2024
- Telefónica, Technology and telecoms policy trends in 2024, 12 January 2024
- Trend Micro, CVE-2023-36025 Exploited for Defense Evasion in Phemedrone Stealer Campaign, 12 January 2024
- UNIT42, Financial fraud APK campaign, 12 January 2024
- CircleID, Internet Governance Outlook 2024: "Win-Win-Cooperation" vs. "Zero Sum Games"?, 14 January 2024
- Security Week, Cloud server abuse leads to huge spike in botnet scanning, 15 January 2024

Upcoming events

- 15-16 January 2024, C-PROC/ PHILIPPINES, (in person), Training of Trainers - training skills and certification programme for CoE judicial trainers, GLACY+, GLACY-e
- 17-23 January 2024, C-PROC/ PHILIPPINES, (in person), Refresher on Introductory course and Advanced Training on Cybercrime and electronic evidence for judges and prosecutors (ToT) , GLACY+, GLACY-e
- 16 January 2024, C-PROC, (online), Contribution to the Steering Committee of the INTERPOL project Momentum in the MENA, CyberSouth+
- 16 January 2024, C-PROC, (online), Meeting with Egypt, Ministry of Justice representatives, to discuss co-operation under CyberSouth+ for the next 3 three years, CyberSouth+
- 16 January 2024, C-PROC, (online), Meeting with US/INL Tunisia to discuss developments in Tunisia and synergies for the period 2024-2026, CyberSouth+
- 19 January 2024, C-PROC, (online), Co-ordination with the EU project ACT Lebanon to discuss the current situation in Lebanon and future steps, CyberSouth+
- 19 January 2024, C-PROC, (online), 7th UN AHC Online preparatory meeting, Octopus, T-CY
- 29 January - 9 February 2024, C-PROC, (in person), Support for participation in the Ad Hoc Committee on new UN Treaty: concluding session, GLACY+, GLACY-e
- January 2024, C-PROC, (online), further developments of the Octopus platform, Octopus
- January 2024, C-PROC, (online), further developments of the CYBOX platform, Octopus
- January 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