Cybercrime Digest

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

01 – 15 April 2024

Source: Council of Europe

Date: 11 April 2024

Ten years of cooperation between Romania and the Council of Europe for capacity building on cybercrime

"The Cybercrime Programme Office of the Council of Europe (C-PROC), based in Bucharest, celebrates this month 10 years since it was founded. On this occasion, on 11 April 2024 an event was organised in Bucharest with representatives of criminal justice authorities in Romania and other relevant institutions to discuss challenges they are facing as well as the way C-PROC can contribute to their capacity building. Romania is constantly supporting activities of this Office, by sharing experience, promoting international standards in the field of cybercrime, as well as in developing an international community of professionals." READ MORE

RELATED ARTICLES:

Council of Europe, Exchange of views with the diplomatic community and international organisations in Bucharest on the occasion of C-PROC's 10th anniversary, 12 April 2024

Council of Europe, C-PROC activity report for 2023, 05 April 2024

Source: RFI

Date: 12 April 2024

JO 2024: les pirates du web promettent un «blackout» pendant le grand événement

"La France s'attend à un déferlement de cyberattaques pendant les Jeux olympiques de Paris, qui se dérouleront du 26 juillet au 11 août 2024. Les autorités chargées de la sécurité de l'espace informationnel français redoutent des offensives informatiques massives, qui seraient lancées directement par la Russie ou par l'intermédiaire de leurs partisans. Et sans surprise, ces offensives cyber qualifiées d'étatiques ont déjà commencé ! Plusieurs sites web de ministères français ont subi les attaques des pirates informatiques prorusses se réclamant du gang Anonymous Soudan." READ MORE

RELATED ARTICLES:

Le Monde, Cyberattaques, arnaques et désinformation, les menaces en ligne qui pèsent sur les Jeux olympiques de Paris, 10 April 2024

Bitdefender, The 'Vote for My Team' Scam Is One Way to Lose Your Steam Account to Criminals, 09 April 2024

Source: Security Affairs

Date: 03 April 2024

Serious security breach hits EU police agency

"The website Politico reported that the Europol has suffered a serious security breach, a batch of sensitive files of top law enforcement officials, including Europol Executive Director Catherine De Bolle, went missing last summer. […] The disappearance of personal files of EUROPOL officials poses a serious risk to the impacted individuals and to the agency's operations, including its investigations. […] It is still unclear how long the files have been missing or which are the cause of the security breach." READ MORE

Source: Phys Org

Date: 10 April 2024

Most cybercriminal threats are concentrated in just a few countries, new index shows

"The researchers used the survey results to construct the novel World Cybercrime Index, enabling comparison between countries. It suggests that cybercriminal threats are primarily concentrated in a small number of countries, with China, Russia, Ukraine, the US, Romania, and Nigeria ranking in the top 10 for each of the five categories." READ MORE

Source: Europol

Date: 05 April 2024

Europol report identifies the most threatening criminal networks in the EU

"All EU Member States and 17 of Europol's partner countries contributed data to identify the most threatening criminal networks in Europe. This resulted in a unique dataset of 821 highest-risk criminal networks, with extensive information on all aspects that describe them and help assess their threat." READ MORE

RELATED ARTICLES: Europol, Decoding the EU's most threatening criminal networks, 05 April 2024

RFI, Europol report identifies more than 800 criminal networks in EU, 05 April 2024

Source: Eurojust

Date: 12 April 2024

Eurojust helps tackle massive fraud of EUR 645 million with medicinal cannabis plants across Europe

"In Germany, France and Spain alone, over 4 500 victims have lodged formal complaints against the fraudsters, who set up a crowd-funding programme to raise a minimum of EUR 50 per investor for the development of medicinal cannabis plants. […] In total, around 550 000 participants worldwide were registered as online investors, most of them European citizens. Around 186 000 participants transferred funds, either via cryptocurrencies or bank transfers." READ MORE

RELATED ARTICLE:

Europol, 9 arrests in EUR 645 million JuicyFields investment scam case, 12 April 2024

Source: Infosecurity

Date: 15 April 2024

Hope Revived for UN Cybercrime Treaty as Negotiations Set to Resume

"A glimmer of hope remains for the UN's proposed Cybercrime Treaty as negotiations look to resume this summer after being on hold in New York since February. However, experts still question if the Russia-led resolution will become a helpful tool in the fight against cybercrime or an unfortunate ally to authoritarian regimes. […] The Treaty is also a way for Moscow to push for an alternative to the 2004 Convention on Cybercrime (aka the Budapest Convention), a similar initiative drawn up by the Council of Europe. […] The next official negotiations are set to take place in New York in the summer of 2024." READ MORE

Source: Euractiv

Date: 11 April 2024

EU Parliament votes to strengthen GDPR enforcement

"Members of the European Parliament voted on Wednesday (10 April) on amendments to strengthen the enforcement of the EU's General Data Protection Regulation (GDPR), however, stakeholders urged for further improvements, particularly regarding complainants' rights and cross-border matters. […] Among other things, the passed amendments to the EU's landmark data protection regulation change the role of the supervisory authorities and remove some of their obligations to share preliminary findings. […] The new Parliament will follow up on the file after the European Elections on 6-9 June." READ MORE

Source: European Parliament

Date: 10 April 2024

Child sexual abuse online: current rules extended until April 2026

"With 469 in favour, 112 against and 37 abstentions, MEPs endorsed a temporary extension of the current e-Privacy derogation that allows the voluntary detection, by internet platforms, of child sexual abuse material (CSAM) online. The derogation will be extended until 3 April 2026 so that an agreement on the long-term legal framework to prevent and combat child sexual abuse online can be reached. […] Rapporteur Birgit Sippel (S&D, Germany) said: « Child sexual abuse is a horrible crime and we need to prevent its spread online. For this reason, we have agreed to extend the derogation that allows some companies to use technology to detect online child sexual abuse material. »" READ MORE

RELATED ARTICLE:

IWF, AI-Generated Child Abuse Sexual Imagery Threatens to "Overwhelm" Internet, 15 April 2024

Source: Tech Business News

Date: 15 April 2024

AI-Powered Cyber Attacks – The Alarming 85% Global Surge

"[…] Cybercriminals are increasingly utilizing AI to enhance their ability to crack users' passwords. Conventionally, hackers relied on brute force algorithms, systematically testing passwords until discovering the correct one. […] State and non-state actors, both skilled and less proficient, are increasingly leveraging AI to enhance their cyber capabilities, posing a significant challenge to cybersecurity efforts globally. […] According to KnowBe4, at least 70% of malicious breaches stem from social engineering or phishing attacks. That means that attackers don't necessarily exploit a technical vulnerability at all, but instead persuade users to surrender their legitimate access credentials." READ MORE

RELATED ARTICLES:

The Record, Cybercriminals are spreading malware through Facebook pages impersonating AI brands, 04 April 2024

IT Security Guru, A Quarter of UK Business Are Not Using AI to Bolster Cybersecurity, 10 April 2024

Source: Council of Europe

Date: 05 April 2024

SLAPPS: abusive lawsuits aimed at silencing journalists must be stopped

"Alarmed by the chilling effect that abusive lawsuits have on freedom of expression and public participation, the Committee of Ministers has issued a Recommendation to its 46 member states aimed at countering the use of strategic lawsuits against public participation (SLAPPs), often used against journalists and media as well as other public watchdogs. […] The recommendation interprets public participation and public interest broadly, extending it to everyone's democratic right to participate in public debate and public affairs, online and offline." READ MORE

Source: Varsity

Date: 15 April 2024

Journalism in the Digital Age: Safeguarding Newsrooms Against Cyber Threats

"According to a study by the International Center for Journalists, which included 714 participants, an alarming 73% of female journalists have reported experiencing violence online. iWatch Africa found that journalists in Ghana faced over 5,000 incidents of online harassment and abuse in the year 2020 alone. […] The 2023 "Freedom in the World" report marks its 50th year by highlighting a troubling trend: a 17-year consistent decline in global freedom. Journalists, serving as vital custodians of truth, now grapple with increasingly complex cyber challenges. These range from phishing and hacking to surveillance and online harassment. Such risks are magnifying one of journalism's pressing issues today: maintaining credibility." READ MORE

RELATED ARTICLES:

Liberainformazione, 30 giorni per la libertà di stampa. Continua la campagna di Amnesty, 12 April 2024

Botasot, Oms: il cyberbullismo colpisce 1 studente su 6, 12 April 2024

Source: Segurilatam

Date: 15 April 2024

Latinoamérica y Caribe sufrieron 200.000 millones intentos de ciberataques en 2023

"Las regiones de Latinoamérica y el Caribe sufrieron, el pasado año, 200.000 millones de intentos ciberataques en 2023. Es decir, un 14,5 por ciento respecto al nivel global. Los países con mayor actividad fueron México, Brasil y Colombia. Así lo ha dado a conocer Fortinet en su último estudio. […] En cuanto al ransomware, desde Fortinet advierten que las detecciones de este malware han disminuido, pero son cada vez más específicos y dirigidos debido al incremento de la sofisticación en las tácticas, técnicas y procedimientos de los ciberdelincuentes." READ MORE

RELATED ARTICLES:

Manage Engine, Los países más atacados de LATAM según IBM, 05 April 2024

Recursos Humanos, Los ciberataques se dispararon en México y Latinoamérica durante el 2023, 03 April 2024

Ionix LATAM, Los 7 fraudes en línea que más afectan en LATAM, 09 April 2024

Source: Crypto News

Date: 02 April 2024

Cybercrime group TA558 strikes phishing campaign against Latin America-based companies

"Threat actor TA558 has launched a new phishing campaign targeting Latin American sectors with Venom RAT, amid rising cyber threats exploiting DarkGate and malvertising. Cybergang TA558 is once again targeting Latin American companies and government agencies in what appears to be a massive phishing campaign aimed at installing Venom RAT, a remote access trojan. […] According to Tarab, the latest attack chain utilizes phishing emails as the primary means of initial access, with Venom RAT being dropped subsequently. […] TA558, known for its activities since at least 2018, has a history of focusing on entities within the Latin America region, employing a range of malware including Loda RAT, Vjw0rm, and Revenge RAT." READ MORE

Source: Crypto ID

Date: 04 April 2024

Ataques às cidades inteligentes e prisão de mais de 400 hackers. Relatório inédito de cibersegurança relaciona principais eventos no mundo

"O cenário de cibersegurança do último ano foi marcado por eventos que destacaram a sofisticação dos criminosos cibernéticos. Desde ataques em larga escala a instituições financeiras até violações massivas de dados comprometendo a privacidade de milhões, a dinâmica dos crimes cibernéticos se revelou desafiadora. […] Um exemplo é a ocorrência de ataques de negação de serviço (DDoS), especialmente com a técnica HTTP/2 Rapid Reset, conforme apontou o relatório recentemente divulgado pela Cloudflare. Destaque para o maior ataque registrado, mitigado pela Google em outubro de 2023, com mais de 398 milhões de requisições por segundo." READ MORE

Source: Council of Europe

Date: 08-12 April 2024

GLACY-e and Octopus Projects: The first pool of national judicial trainers of Brazil finalise the training programme on cybercrime and electronic evidence

"A group of 19 prosecutors from several regions of Brazil underwent the advanced training course on cybercrime and electronic evidence from 8 to 12 April 2024, at the Prosecutor's Office in São Paulo. The course was organised by the Federal Public Ministry of Brazil with the support of the GLACY-e and Octopus projects, aiming at reinforcing the pool of national trainers able to pass on their knowledge on cybercrime and e-evidence to their peers and to enhance therefore the country's criminal justice response." READ MORE

RELATED ARTICLE:

Ministério Público Federal, Procuradores participam de capacitação sobre combate a crimes cibernéticos promovida pelo Conselho da Europa, 15 April 2024

Source: Electronic Frontier Foundation

Date: 01 April 2024

Ola Bini Faces Ecuadorian Prosecutors Seeking to Overturn Acquittal of Cybercrime Charge

"Ola Bini, the software developer acquitted last year of cybercrime charges in a unanimous verdict in Ecuador, was back in court last week in Quito as prosecutors, using the same evidence that helped clear him, asked an appeals court to overturn the decision with bogus allegations of unauthorized access of a telecommunications system. […] Bini's acquittal was a major victory for him and the work of security researchers. By assessing the evidence presented, the court concluded that both the Prosecutor's Office and CNT failed to demonstrate a crime had occurred. There was no evidence that unauthorized access had ever happened, nor anything to sustain the malicious intent that article 234 of Ecuador's Penal Code requires to characterize the offense of unauthorized access." READ MORE

Source: La Republica

Date: 15 April 2024

Costa Rica: Países no adheridos al convenio de Budapest no van a impedir cerrar un ciclo de ciberataques

"Alianza con Estados Unidos permitirá un nivel más alto de monitoreo para prevenir amenazas del que ya se tenía planeado. […] Costa Rica ratifica el Convenio de Budapest en el 2017, que es un instrumento legal que nosotros podemos y debemos de hacer uso porque nos ayuda en investigaciones forenses con la cooperación de otros países y en dar aprehensión a los hackers; no se vale que, por países que no se comprometan a firmar este convenio, no podamos cerrar un ciclo de ciberataques." READ MORE

Source: The Herald

Date: 02 April 2024

Africa needs robust legal framework to fight cybercrime

"Although the African Union has made significant efforts to combat cybercrime through initiatives such as the African Union's Convention on Cyber Security and Data Protection Laws, the continent still faces notable challenges. […] Tech related scams and their implications for law enforcement, regulators, and the general population in Africa are also a cause for concern." READ MORE

Source: Le 360, Afrique

Date: 01 April 2024

Réglementation des crypto-monnaies: où en sont les 4 pays africains à taille critique, selon le GAFI

"[…] L'Afrique n'est pas épargnée par les risques croissants liés aux actifs virtuels et leurs services associés. Le récent rapport du Groupe d'action financière (GAFI) met en lumière les efforts déployés par les juridictions ayant sur leur territoire une activité de fourniture de services d'actifs virtuels (VASP) d'importance matérielle pour se conformer à la Recommandation 15 sur leur réglementation (voir plus bas). En Afrique, il n'y a que quatre pays éligibles à cette condition. Il s'agit du Nigéria, l'Afrique du Sud, l'Égypte et les Seychelles. Les 50 autres pays du continent n'ont pas encore atteint la taille critique requise pour être pris en compte." READ MORE

Source: Africa Cybersecurity Magazine

Date: 02 April 2024

Protection des données publiques : Le Président demande la préparation d'un nouveau projet de loi au Sénégal

"Le nouveau Président du Sénégal, Bassirou Diomaye FAYE s'engage pour sécuriser les données publiques dans un contexte de numérisation croissante des services gouvernementaux dans le pays. Pour cause, lors du conseil des Ministres du mercredi 17 avril 2024, il a demandé au Ministre de l'Économie Numérique, Alioune SALL, de préparer un projet de loi pour la protection des données issues des administrations publiques." READ MORE

Source: Business Day

Date: 07 April 2024

How unemployment fuels cybercrime in Nigeria

"In the wake of escalating youth unemployment, a disconcerting trend is surfacing— a surge in cybercrime and a resurgence of voodoo practices. This unsettling correlation between economic distress and unconventional criminal activities underscores the pressing challenges faced by the younger generation. You do not need to travel far across Nigeria to see a generation of young people lost in the world of cybercrime and ostensibly inspired by the likes of Hushpuppi. You will find them in many Nigerian cities like Lagos, Benin and Owerri, and even up to Accra, Johannesburg, Dubai and Kuala Lumpur. […] Some of these cyber criminals did not complete their education while others are high school graduates or even students. Many address themselves as 'yahoo boys' – a known term in Nigeria for cyber criminals, suggesting that they are unashamed of their practices. Those in Accra describe their enterprise as a 'pressing computer'." READ MORE

Source: IT Web Africa

Date: 05 April 2024

Equatorial Guinea edges closer to passing cybercrimes law

"Equatorial Guinea is moving closer to passing a cybersecurity law after its parliament, this week, accepted articles defining computer crimes and other cybercrimes, as well as penalties and fines that would be imposed on those who commit them." READ MORE

RELATED ARTICLE:

African Business, Equatorial Guinea: Adoption of articles defining computer crime and cybercrime, 03 April 2024

Source: Le Faso

Date: 02 April 2024

Burkina/Lutte contre la cybercriminalité : Deux présumés cybers délinquants mis aux arrêts

"Ce groupe était impliqué dans des cas d'usurpation d'identité suivie de vols de numéraire via les Technologies de l'Information et de la Communication (TIC), en utilisant des numéros préalablement obtenus à partir de Cartes Nationales d'Identité Burkinabé (CNIB) égarées. Ces numéros étaient ensuite utilisés pour recevoir frauduleusement des transactions financières découlant de leurs activités illégales." READ MORE

Source: The Eastleigh Voice

Date: 12 April 2024

Kenya: Parliament approves new cybersecurity regulations

"The National Assembly has approved the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations of 2024, which enhance the enforcement of the laws established in 2018. […] Among the objectives of the new regulations are the establishment of a framework for monitoring, detecting, and responding to cybersecurity threats within Kenya's cyberspace and the creation of a structure for the setup and administration of cybersecurity operations centres." READ MORE

Source: INTIC

Date: 10 April 2024

Moçambique testa capacidade de resposta à incidentes cibernéticos

"O Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) IP. realizou […] a primeira edição do Exercício Internacional de Cibersegurança, dedicado ao sector da energia,entre Moçambique, Cabo Verde e Portugal, com o objectivo de testar capacidades de resposta à incidentes cibernéticos e fortalecer a cooperação internacional entre as diferentes entidades responsáveis pela cibersegurança." READ MORE

Source: BBC

Date: 10 April 2024

Zambia uncovers 'sophisticated' Chinese cybercrime syndicate

"A « sophisticated internet fraud syndicate » has been uncovered in Zambia, leading to the arrest of 77 people, including 22 Chinese nationals. It was a « significant breakthrough in the fight against cybercrime », the authorities said after a multi-agency raid on a Chinese-run company. The firm employed Zambians who believed they were to be call-centre agents." READ MORE

RELATED ARTICLE:

Dark Reading, Zambia Busts 77 People in China-Backed Cybercrime Operation, 11 April 2024

Source: The Mercury

Date: 01 April 2024

First Tasmanian man jailed over AI-generated child abuse material after AFP and Tasmania Police raid

"A Tasmanian man has likely become the first person in the state's history to be jailed over AI-generated child abuse material. […] The investigation came about after TAS-JACET received « multiple reports » that an Australian-based user was saving and downloading child abuse material from a website and social media platform. […] « Child abuse material is still child abuse material, no matter what form it takes, » Det Sgt Hardcastle said. « People may not be aware that online simulations, fantasy, text-based stories, animations and cartoons, including artificial intelligence-generated content depicting child sexual abuse are all still considered child abuse material under Commonwealth legislation.»." READ MORE

Source: Beeping Computer

Date: 13 April 2024

Firebird RAT creator and seller arrested in the U.S. and Australia

"A joint police operation between the Australian Federal Police (AFP) and the FBI has led to the arrest and charging of two individuals who are believed to be behind the development and distribution of the « Firebird » remote access trojan (RAT), later rebranded as « Hive ». Firebird/Hive aren't among the most widely recognized and deployed RATs out there, but they could still have impacted users' securitys worldwide. […] The indictment alleges that Chakhmakhchyan promoted Hive's stealthy access to target computers to an undercover FBI agent, to whom he sold a license. In a separate case, a buyer clearly told the seller his goals were to steal $20k worth of Bitcoin and $5k worth of documents, leaving no doubts about the intention to use the tool for illegal activities." READ MORE

Source: AsiaNews Network

Date: 01 April 2024

Philippines faces more cyberattacks from China-based hackers

"The Philippines faces growing cyberthreats from the exploitation of generative artificial intelligence (GenAI) and continuous targeting by China-backed cyberthreat actors, Texas-based cybersecurity firm CrowdStrike said in its 2024 Global Threat Report. The report highlights how AI tools that can generate increasingly convincing text, images and video are making it easier for threat actors to spread misinformation and access sensitive systems. […] The report cautions that « Chinese, Russian and Iranian adversaries will likely conduct misinformation and disinformation operations with GenAI tools. »" READ MORE

Source: VOA News

Date: 08 April 2024

Experts fear Cambodian cybercrime law could aid crackdown

"The Cambodian government is pushing ahead with a cybercrime law experts say could be wielded to further curtail freedom of speech amid an ongoing crackdown on dissent. […] Digital rights and legal experts who reviewed the law told VOA that its vague language, wide-ranging categories of prosecutable speech and lack of protections for citizens fall short of international standards, instead providing the government more tools to jail dissenters, opposition members, women and LGBTQ+ people." READ MORE

Source: Global Witness

Date: 02 April 2024

"Votes will not be counted": Indian election disinformation ads and YouTube

"To test YouTube's treatment of election disinformation in India, Access Now and Global Witness submitted 48 advertisements in English, Hindi, and Telugu containing content prohibited by YouTube's advertising and elections misinformation policies. YouTube reviews ad content before it can run, yet the platform approved every single ad for publication. […] The policy appears not to have been implemented in the process of reviewing ads. For example, the policy suggests that YouTube will remove misinformation that has the effect of suppressing voting and even provides a specific example of such prohibited content. In our test, we submitted the same type of content, and YouTube approved it for publication […]." READ MORE

Source: Toute la Thaïlande

Date: 11 April 2024

Pourquoi la Thaïlande n'arrive pas à mettre fin à la cybercriminalité ?

"Malgré les tentatives de la Thaïlande pour réprimer la cybercriminalité, le nombre de cas et les dommages n'ont toujours pas diminué. Le ministre de l'Économie et de la société numériques (DES), attribue l'incapacité à contrôler les escroqueries en ligne au fait que les gangs utilisent des stratégies de plus en plus sophistiquées. […] le nombre de cas de cybercriminalité reste constant et les dommages s'élèvent en moyenne à 100 millions de bahts (2,54 millions d'euros) par jour." READ MORE

Source: Tech Crunch

Date: 12 April 2024

How Ukraine's cyber police fights back against Russia's hackers

"Ukraine's cyber police talks crypto, ransomware and documenting war crimes after Russia's invasion. […] That includes tracking what war crimes Russian soldiers are committing in the country, which they sometimes post on social media; monitoring the flow of cryptocurrency funding the war; exposing disinformation campaigns; investigating ransomware attacks; and training citizens on good cybersecurity practices." READ MORE

RELATED ARTICLE:

Babel, Law enforcement officers identified the hackers who hacked "Kyivstar". The materials will be handed over to the International Criminal Court, 04 April 2024

Source: CBS News

Date: 14 April 2024

Criminal exploits of Scattered Spider earn respect of Russian ransomware hackers

"In the shadowy corners of the dark web, young hackers from the U.S., U.K., and Canada met and teamed up with Russian ransomware hackers, becoming powerful partners in crime.[…] Their criminal exploits have caught the attention of cybersecurity companies and earned the respect of other criminal hackers, including one of the most notorious Russian ransomware gangs, BlackCat, also known as ALPHV, who saw the young, native-English-speaking Westerners as a potential « force multiplier » for their ransomware attacks." READ MORE

Source: ProofPoint

Date: 10 April 2024

Security Brief: TA547 Targets German Organizations with Rhadamanthys Stealer

"Proofpoint identified TA547 targeting German organizations with an email campaign delivering Rhadamanthys malware. This is the first time researchers observed TA547 use Rhadamanthys, an information stealer that is used by multiple cybercriminal threat actors. Additionally, the actor appeared to use a PowerShell script that researchers suspect was generated by large language model (LLM) such as ChatGPT, Gemini, CoPilot, etc. Emails sent from the threat actor impersonated the German retail company Metro purporting to relate to invoices." READ MORE

Source: The Guardian

Date: 04 April 2024

UK: Police launch inquiry after MPs targeted in apparent 'spear-phishing' attack

"A police investigation has been launched after MPs were apparently targeted in a "spear-phishing" attack, in what security experts believe could be an attempt to compromise parliament. A police force said it had started an inquiry after receiving a complaint from an MP who was sent a number of unsolicited messages last month. Twelve people working in Westminster, including a serving government minister, told Politico they had received unsolicited WhatsApp messages from two suspicious mobile numbers in the past six months." READ MORE

Source: The Hacker News

Date: 03 April 2024

U.S. Cyber Safety Board Slams Microsoft Over Breach by China-Based Hackers

"The U.S. Cyber Safety Review Board (CSRB) has criticized Microsoft for a series of security lapses that led to the breach of nearly two dozen companies across Europe and the U.S. by a China-based nation-state group called Storm-0558 last year. The findings, released by the Department of Homeland Security (DHS) on Tuesday, found that the intrusion was preventable, and that it became successful due to a « cascade of Microsoft's avoidable errors ». […] As many as 60,000 unclassified emails from Outlook accounts are believed to have been exfiltrated over the course of the campaign that began in May 2023. China has rejected accusations that it was behind the attack." READ MORE

RELATED ARTICLE:

The Verge, Microsoft could have prevented Chinese cloud email hack, US cyber report says, 03 April 2024

Source: The Record

Date: 09 April 2024

Medusa cybercrime gang takes credit for another attack on US municipality

"The Tarrant County Appraisal District — which determines property values for tax purposes in the Fort Worth area — confirmed to Recorded Future News two weeks ago that it was a victim of a ransomware attack. On Monday, the Medusa cybercrime gang took credit for the incident, threatening to leak nearly 218 gigabytes of data in six days if a $100,000 ransom is not paid. […] In addition to the Tarrant County incident, the Medusa gang recently attacked the government of an Illinois county on the border with Iowa." READ MORE

Source: US Department of Justice

Date: 12 April 2024

Delaware Woman Arrested for International Sextortion and Money Laundering Scheme

"According to an indictment unsealed today, from May 2020 through December 2022, Hadja Kone, 28, of Wilmington, and Siaka Ouattara, 22, of Abidjan, Cote d'Ivoire, and other co-conspirators allegedly operated an international, financially motivated sextortion and money laundering scheme in which the conspirators engaged in cyberstalking, interstate threats, money laundering, and wire fraud. […] The FBI is investigating the case, with assistance from the government of Cote d'Ivoire." READ MORE

Latest reports

- Ministerio Publico Federal, Brasil, MPF reúne em livro conhecimento científico e experiência de investigadores de crimes com criptoativos, 2024
- Help Net Security, Escalating malware tactics drive global cybercrime epidemic, 01 April 2024
- Security Week, AI Hallucinated Packages Fool Unsuspecting Developers, 01 April 2024
- Developpez, Un courriel de phishing sur six est ouvert et le phishing par lien a été une réussite dans 11 % des cas, 02 April 2024
- CheckPoint, Agent Tesla Targeting United States & Australia: Revealing the Attackers' Identities, 02 April 2024
- Sucuri, Magento Shoplift: Ecommerce Malware Targets Both WordPress & Magento CMS, 02 April 2024
- Checkpoint, Beyond Imagining – How Ai Is Actively Used In Election Campaigns Around The World, 02 April 2024
- Canal AR, ¿Cuál es el rol de la inteligencia artificial en la ciberseguridad en Argentina y Latinoamérica?, 04 April 2024
- TechTarget, Cloud computing forensics techniques for evidence acquisition, 02 April 2024
- CNIL, The economic impact of GDPR, 5 years on, 02 April 2024
- CISA, ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System, 02 April 2024
- Forensic, Presenting Digital Evidence that Holds up in Court, 03 April 2024
- Krebs on Security, 'The Manipulaters' Improve Phishing, Still Fail at Opsec, 03 April 2024
- ProofPoint, Threat Actors Deliver Malware via YouTube Video Game Cracks, 03 April 2024
- Sophos, Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector, 03 April 2024
- France Verif, La hausse de la cybercriminalité n'est pas un fantasme : les piratages multipliés par 7 depuis 2020, 03 April 2024
- Resecurity, The New Version Of JsOutProx Is Attacking Financial Institutions In APAC And MENA Via GitLab Abuse, 03 April 2024
- Enisa, Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis, 04 April 2024
- Hack Read, New Red Ransomware Group (Red CryptoApp) Exposes Victims on Wall of Shame, 04 April 2024
- FBI, FBI Releases Internet Crime Report, 04 April 2024
- 01Net, Ransomware: le retour des pirates de Lockbit est compromise, 04 April 024
- Cisco Talos, CoralRaider targets victims' data and social media accounts, 04 April 2024
- ProofPoint, Latrodectus: This Spider Bytes Like Ice, 04 April 2024
- Fortinet, Byakugan – The Malware Behind a Phishing Attack, 04 April 2024
- Securityaffairs, Ivanti Fixed For 4 New Issues in Connect Secure And Policy Secure, 04 April 2024
- Krebs on Security, Fake Lawsuit Threat Exposes Privnote Phishing Sites, 04 April 2024
- Dinamo Networks, Ciberataques dobram em cinco anos, selecionam vítimas e miram CEOs, 04 April 2024

- Help Net Security, 76% of consumers don't see themselves as cybercrime targets, 04 April 2024
- Deep Instinct, DarkBeatC2: The Latest MuddyWater Attack Framework, 04 April 2024
- Microsoft, Same targets, new playbooks: East Asia threat actors employ unique methods,04 April 2024
- Medianama, Voice Cloning Scams: The Alarming Use Of Artificial Intelligence By Cybercriminals, 05 April 2024
- Help Net Security, Cybercriminal adoption of browser fingerprinting, 05 April 2024
- Medium, Don't Trust the Cache: Exposing Web Cache Poisoning and Deception vulnerabilities, 05 April 2024
- The Den, Mercer University, How to avoid becoming a victim of cybercrime, according to Mercer experts, 05 April 2024
- Techspective, The Clock is Ticking to Protect Vulnerable Groups from AI-Driven Cybercrime, 05 April 2024
- Numerama, Qui est la cible favorite des hackers parmi vos collègues, 07 April 2024
- Securityaffairs, Over 92,000 Internet-Facing D-Link Nas Devices Can Be Easily Hacked, 07 April 2024
- B2B Cyber Security, Ransomware: Cybercrime Groups Increase Ransom Demands, 07 April 2024
- Cybersecurity, 10 Strategies to Fortify SCADA System Security, 08 April 2024
- Fortinet, ScrubCrypt Deploys VenomRAT with an Arsenal of Plugins, 08 April 2024
- The Hacker News, The Drop in Ransomware Attacks in 2024 and What it Means, 08 April 2024
- Chainanalysis, What You Need to Know About the Bitcoin Halving, 09 April 2024
- Black Berry, Top 20 MITRE ATT&CK Tactics Threat Actors Use Now, 09 April 2024
- European Data Protection Supervisor, Annual Report 2023: adaptability in a changing world, 09 April 2024
- IT Security, Lei do Cibercrime: no compasso das ameaças digitais, 09 April 2024
- Flatt Security, BatBadBut: You can't securely execute commands on Windows, 09 April 2024
- Sysdig, RUBYCARP: A Detailed Analysis of a Sophisticated Decade-Old Botnet Group, 09 April 2024
- Unit 42, Muddled Libra's Evolution to the Cloud, 09 April 2024
- PDucklin, Fallout from XZ/SSH supply chain attack continues, 10 April 2024
- The Hacker News, Researchers Uncover First Native Spectre v2 Exploit Against Linux Kernel, 10 April 2024
- Help Net Security, WEF Cybercrime Atlas: Researchers are creating new insights to fight cybercrime, 10 April 2024
- CISA, CISA Announces Malware Next-Gen Analysis, 10 April 2024
- WeLeaveSecurity, eXotic Visit campaign: Tracing the footprints of Virtual Invaders, 10 April 2024
- Trend Micro, Cyberespionage Group Earth Hundun's Continuous Refinement of Waterbear and Deuterbear, 11 April 2024
- Security Leaders, IA maliciosa e ataque aos dados são duas das tendências do Cibercrime em 2024, 11 April 2024
- Silicon, Cibercriminosos abusaram do protocolo de RDP, 11 April 2024

- Reuters, Apple drops term 'state-sponsored' attacks from its threat notification policy, 11 April 2024
- The Register, 96% of US hospital websites share visitor info with Meta, Google, data brokers, 11 April 2024
- Sucuri Blog, Credit Card Skimmer Hidden in Fake Facebook Pixel Tracker, 11 April 2024
- Claroty, TEAM82, Unpacking the Blackjack Group's Fuxnet Malware, 12 April 2024
- Internet Safety Statistics, How Ethical Hacking Practices Are Affected by the Legislation, 13 April 2024
- 9to5 MAC, Security Bite: Annual cost of cybercrime to hit $9.2 trillion in 2024, 14 April 2024
- Asia Business Law Journal, Analysis of AI regulatory frameworks in South Korea, 15 April 2024
- Orbis News, O Varejo brasileiro na mira do cibercrime. Por Denis Furtado, 15 April 2024
- CiberPrisma, Aumento récord en pérdidas por Ciberdelitos en 2023: Informe del FBI revela impacto alarmante, 15 April 2024
- Simpli Learn, 20 Emerging Cybersecurity Trends to Watch Out in 2024, 15 April 2024
- Economis, Ciberataques y ransomware en América Latina: Amenazas y estrategias de protección, 15 April 2024
- AAG IT, The Latest 2024 Cyber Crime Statistics (updated April 2024), April 2024
- ENISA, AR-in-a-Box: Cybersecurity Awareness Raising: The ENISA-Do-It-Yourself Toolbox, 2024

Upcoming events

- 15-17 April 2024, C-PROC/MAURITANIA, (in person), Advisory mission on cybercrime legislation, Octopus, GLACY-e
- 15-17 April 2024, C-PROC/AUSTRIA, (in person), Support for participation in the informal meeting - UN AHC, GLACY-e
- 16-18 April 2024, C-PROC/CAMEROON, (online), Introductory course on Budapest Convention for the task force involved in the legislative reform on cybercrime and electronic evidence, GLACY-e
- 17-18 April 2024, C-PROC/ITALY, (in person), Support for participation in the Cyber Crime Conference, GLACY-e
- 17-18 April 2024, C-PROC/PORTUGAL, (in person), Launching event of CyberSouth+, T-CY, CyberSouth+
- 18 April 2024, T-CY/CZECH REPUBLIC, (in person), Final Conference, T-CY
- 23 April 2024, C-PROC/PANAMA, (online), Workshop on the legislative reform on cybercrime, GLACY-e
- 22-26 April 2024, C-PROC/ROMANIA, Contribution to the 35th General Assembly of the European Youth Information and Counselling Agency, C-PROC
- 24-26 April 2024, C-PROC/LESOTHO, (online), Introductory course on Budapest Convention for the drafting team involved in the legislative reform on cybercrime and electronic evidence, GLACY-e
- 23-25 April 2024, C-PROC/KOSOVO*, (in person), Domestic Specialised Judicial Training Course on International Cooperation on cybercrime and electronic evidence, CYBERKOP, Octopus (*All

references to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations' Security Council Resolution 1244 and without prejudice to the status of Kosovo)

- 23-25 April 2024, C-PROC/JORDAN, (in-person), Visit to Jordan to discuss the new cybercrime legislation and the national interest in the Budapest Convention, CyberSouth+
- 25 April 2024, C-PROC, (online), Contribution to the launching conference of the EUROMED JUSTICE Project VI, CyberSouth+
- By 26 April 2024, C-PROC/SIERRA LEONE, (desk study), Support for the legislative process on data protection, GLACY-e
- 29-30 April, C-PROC/ECUADOR, (online), Data protection workshop for LEAs and prosecutors, GLACY-e
- 30 April 2024, C-PROC/GLOBAL, Fourth series of peer-to-peer webinars in the framework of the International Network of Judicial Trainers (theme: cyberviolence), GLACY-e
- 29 April – 03 May 2024, NIGERIA, (in person), Support for the 10th Africa Working Group meeting on Cybercrime for Heads of Units, GLACY-e
- April – June 2024, C-PROC, (research), Regional study on legislation in Southeast Asia countries, 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