Cybercrime Digest

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

16 – 31 December 2022

Source: Council of Europe

Date: 16 December 2022

iPROCEEDS-2: New guide for criminal investigations of ransomware attacks

"A new tool is now available to facilitate more effective criminal justice responses to the rising threat of ransomware. The "Guide for criminal investigations of ransomware attacks" […] focuses on the investigative steps to be followed, the legal framework, the collection of evidence, cooperation with service providers and international cooperation. […] The Guide has been prepared under the iPROCEEDS-2 joint project of the Council of Europe and the European Union. It complements the Budapest Convention on Cybercrime and its Second Additional Protocol as well as the Guidance Note adopted by the Cybercrime Convention Committee in November 2022." READ MORE

Source: Gadget

Date: 30 December 2022

How cybercrime evolved in 2022 – and the lessons learned

"In June 2022, the Costa Rican government was forced to declare a national emergency after a significant ransomware attack by Conti, a hacking group with Russian ties. The group had found vulnerabilities within the public sector cybersecurity infrastructure which left many agencies struggling to regain their feet, and many citizens seriously affected by the outages and shortages. The sheer scale of this attack and the magnitude of its impact on society, people and business, underscored the growing complexity of the cybercrime landscape and the threats it represents. One of the key lessons learned in 2022 is how every layer of society and business can be affected by a successful cyber attack." READ MORE

RELATED ARTICLE:

TechCrunch, Meet the cybercriminals of 2022, 30 December 2022

Source: Forbes (Australia)

Date: 20 December 2022

2022: The year of the data breach

"2022 offered a data security reality check. It was the year of the data breach. And while the proliferation of serious data breaches has shone a light on the need to enhance cybersecurity across […] institutions, organisations and households, it's likely we'll see this trend remain in 2023. At its core, the data theft trend is ultimately a slight pivot from the ransomware tactics we've come to expect." READ MORE

Source: Domain Incite

Date: 20 December 2022

ICANN expects to approve Whois Disclosure System next month

"ICANN could be offering a centralized system for requesting private domain registration data as early as a year from now, a mere five and a half years after GDPR ruined the global Whois system for many. The Org recently alluded to its "board's anticipated January 2023 vote to move forward in implementing the new system to streamline the intake and routing of requests for access to non-public gTLD registration data" in a blog post." READ MORE

Source: Europol

Date: 19 December 2022

14 countries tackle violent extremism online in a coordinated referral action day

"On 15 December 2022, the European Union Internet Referral Unit (EU IRU) at Europol coordinated the second Referral Action Day (RAD) against violent right-wing extremist and terrorist content online. The coordinated action involved specialised units from 14 countries, including 13 EU Member States (MS) and one non-EU country* (Czechia, Denmark, France, Germany, Hungary, Ireland, Italy, Malta, The Netherlands, Portugal, Slovakia, Slovenia, Spain, United Kingdom). The participating authorities were involved in detecting and flagging terrorist content to online service providers and evaluating their responses. The activities resulted in the referral of 831 items to 34 affected platforms. Referred materials include content produced by or favouring proscribed right-wing extremist organisations. It also includes content disseminated in relation to terrorist attacks motivated by violent extremism. Such materials include livestreams, manifestos, claims and celebrations of attacks." READ MORE

Source: Digwatch

Date: 19 December 2022

Users of Ukraine's DELTA military system targets of information stealing malware

"The Computer Emergency Response Team of Ukraine (CERT-UA) revealed that users of the DELTA situational awareness program were receiving phishing emails and instant messages from a compromised email account at the Ukrainian Ministry of Defense. The emails and messages were intended to infect computers with malware that steals information." READ MORE

Source: Tech.co

Date: 22 December 2022

FBI Recommends Using Ad Blockers to Avoid Cybercrime

"In a statement from the FBI […], the agency suggested that internet users download an ad blocker, as cyber criminals adopt more and more sophisticated ways to dupe victims into downloading harmful software or handing over their details. According to the FBI, cyber criminals are purchasing adverts that appear in internet search results, usually masquerading as a legitimate business or service. As these adverts appear at the top of a search page, there is a high chance of an unwitting victim clicking on them, after which they will be redirected to a website which appears to be the real deal but is instead a fraudulent facsimile of the authentic website." READ MORE

Source: CNBC

Date: 16 December 2022

The FBI is worried about a wave of cybercrime against America's small businesses

"As more large businesses and corporations invest in cybersecurity tools, hackers are increasingly targeting small and medium-sized businesses, FBI Supervisory Special Agent Michael Sohn said at CNBC's Small Business Playbook event […].In 2021, the FBI's Internet Crime Complaint Center received 847,376 complaints regarding cyberattacks and malicious cyber activity with nearly $7 billion in losses, the majority of which targeted small businesses." READ MORE

Source: Eurojust

Date: 19 December 2022

Takedown of online investment fraud responsible for losses of EUR 15 million

"With the support of Eurojust, authorities in Italy and Albania have dismantled an online investment fraud involving the use of cryptocurrencies. During an action, EUR 3 million worth of assets were seized. Eurojust supported the judicial cooperation and assisted the authorities in setting up and funding a joint investigation team (JIT). […] The total damage caused is estimated at EUR 15 million. In an action coordinated by Eurojust from 13 to 15 December, precautionary detention orders were executed against the main suspects of the fraud. Thirteen locations were searched in Albania. In Italy and Albania, more than 160 electronic devices (computers, servers and digital video recorders), 1 mobile phone and EUR 3 million worth of assets (including 11 properties) were seized." READ MORE

Source: CNET

Date: 26 December 2022

Cybercriminalité: les gamers et le métavers vont devenir des cibles de choix

"Les experts en cybersécurité s'accordent à dire que 2023 verra l'émergence de menaces ciblant les nouveaux usages dans les domaines du jeu vidéo en ligne, de l'éducation et des métavers. […] L'éditeur de solutions de cybersécurité Kaspersky pense que les cyber délinquants vont s'attaquer à de nouveaux domaines, comme les plateformes de jeu vidéo, les mondes de réalité virtuelle et les technologies utilisées par les enfants pour l'école et les loisirs. Il s'agirait là d'une manière de s'adapter à la vigilance croissante des entreprises et des particuliers qui sont de plus en plus au fait des escroqueries par courrier électronique, par SMS et sur les réseaux sociaux." READ MORE

Source: KrebsonSecurity

Date: 19 December 2022

Hacked Ring Cams Used to Record Swatting Victims

"Two U.S. men have been charged with hacking into the Ring home security cameras of a dozen random people and then "swatting" them — falsely reporting a violent incident at the target's address to trick local police into responding with force. Prosecutors say the duo used the compromised Ring devices to stream live video footage on social media of police raiding their targets' homes, and to taunt authorities when they arrived." READ MORE

Source: Tech Monitor

Date: 16 December 2022

Cybercrime is rampant. ISPs could do more to stop it

"In August 2016, one of the world's largest botnets implemented a distributed denial of service (DDoS) attack that smothered vast swathes of the US internet, including consumer giants like Amazon, Airbnb, Github, HBO, Twitter and Paypal. Dubbed Mirai, this particular horde of bots was made up of hundreds of thousands of smart appliances – binding everything from fridges and kettles, to televisions and baby monitors, to its ferocious will. Mirai was supposed to be a turning point. In the wake of the attack, the FCC published a new set of rules for internet service providers (ISPs) compelling these firms to secure their customers' data against cyberattacks." READ MORE

Source: López-Dóriga Digital

Date: 28 December 2022

Se registran cuatro mil ataques de ransomware al día en América Latina

"En los primeros ocho meses de este año se ha registrado un promedio de cuatro ataques de ransomware al día en América Latina, de acuerdo con cifras de Kaspersky. Aunque esta cifra representa una disminución del 28% en comparación con el mismo periodo de 2021, los expertos advierten que esta reducción no significa que los ciberdelincuentes estén abandonando este método de operación. Al contrario, alertan que los grupos criminales se han enfocado en ataques dirigidos, pues en la región se han detectado familias locales de ransomware cuyo único objetivo es atacar a instituciones latinoamericanas, ya sea del sector público o privado." READ MORE

Source: BusinessTech

Date: 28 December 2022

The world faces a cybercrime catastrophe — including South Africa

"A report published by cybersecurity company Surfshark has highlighted South Africa ranking 6th in the world regarding cybercrime density – which costs the country an estimated R2.2 billion annually. […] Surfshark's cybercrime report for 2021 showed that South Africa had 52 cybercrime victims per one million internet users, with other countries showing even more alarming numbers." READ MORE

Source: WeAreTech Africa

Date: 20 December 2022

Le Tchad élabore sa Stratégie nationale de cybersécurité

"Le Tchad est sur la voie de se doter d'une Stratégie nationale de cybersécurité. Le ministère des Télécommunications et de l'Economie numérique et l'Agence Nationale de Sécurité Informatique et de Certification Electronique (ANSICE) ont procédé, mercredi 14 décembre, au lancement des travaux de l'élaboration de ladite stratégie en présence du ministre en charge des Télécommunications, Mahamat Allahou Taher. Elaborée en partenariat avec l'Union internationale des télécommunications (UIT), la future Stratégie nationale de cybersécurité vise à trouver les moyens permettant de mieux lutter contre toutes formes d'attaques cybernétiques." READ MORE

Source: Morocco World News

Date: 28 December 2022

Morocco Announces Draft Law penalizing Online Defamation

"Morocco is moving to penalize defamation in news reporting and on social media, with the country's Court of Cassation ruling earlier this week for social media posts to be tackled under the Penal Code. The move means Morocco will soon tackle social networks posts including defamation and fake news under the penal code and not the press and publishing code. Minister of Justice Abdellatif Ouahbi announced the news on Monday during a parliamentary session, stressing that a draft law to that regard will soon be submitted to the government. […] As he justified before the parliament the decision to severely punish libel and related violations of individuals' privacy, Minister Ouahbi recalled that Morocco was last year one of the signatories of the Budapest Convention on Cybercrime." READ MORE

Source: La Nation (Benin)

Date: 20 December 2022

Lutte contre la cybercriminalité. Aurélie Adam Soulé Zoumarou propose une thérapie de choc

"A travers son ministre du Numérique et de la Digitalisation, Aurélie Adam Soulé Zoumarou, le Bénin a pris activement part les 15 et 16 décembre derniers à Genève à la 11e édition des Assises de la Transformation digitale en Afrique (Atda). Aux côtés de ses homologues […], elle a apporté sa contribution lors de la session ministérielle autour du thème «Cybersécurité: quels défis pour votre pays?» Pour la ministre du Numérique et de la Digitalisation du Bénin, aucun pays ne peut s'en sortir seul lorsqu'il s'agit des questions de cybersécurité." READ MORE

Source: Life - The Philippine Star

Date: 20 December 2022

How Asia-Pacific has become a top target for online scams, phishing and identity theft

"In 2022, it was found that one in four online shoppers in the Asia-Pacific region became victim of online scams, not only through shopping but also via romance scams. With cybercriminals becoming ever more sophisticated, many people found themselves totally blindsided by these attacks. In an APAC Consumer Cybersecurity Survey, two out of three respondents said they encountered online scams in the last 12 months. The most common types of scam were online shopping (21%), social media (18%), and investment (15%)." READ MORE

RELATED ARTICLE:

PhilStar, Fighting cybercrime together, 26 December 2022

Source: Khmer Times

Date: 16 December 2022

Cambodia: Embracing Cybersecurity in Combating Cybercrime

"October 26th, the Malaysian Business Chamber of Cambodia (MBCC) organised a forum in Sofitel Phnom Penh Phokeethra. The event was presided over by Chea Vandeth, Minister of Post and Telecommunications, and Datuk Eldeen Husaini Mohd Hashim, Malaysian Ambassador to Cambodia. At the Forum, Oknha Tan Khee Meng, president of MBCC, said during his opening remarks that cybersecurity and cybercrimes are heated problems faced by countries, including Cambodia and Malaysia, which thus required extra attention from governments, relevant entities and private sectors to create strong defence to protect data and information." READ MORE

Source: MuySeguridad

Date: 16 December 2022

Estas serán las principales tendencias en ciberdelincuencia en 2023

"A falta de conocer los de este año, según el Informe Ciberamenazas y Tendencias de 2022 elaborado por el CCN-CERT del Centro Criptológico Nacional, en 2021 se detectaron 28.695 vulnerabilidades. Esto supone un 23,31% más respecto a las 23.269 de 2020. La mayoría ellas dirigidas al sector público, entidades bancarias, sanitarias y financieras. 2023 se presenta como un auténtico reto en una tendencia, la de los ciberataques, que no hace otra cosa que crecer ejercicio tras ejercicio." READ MORE

Source: El Independiente

Date: 25 December 2022

Radiografía de la década de la ciberdelincuencia en España

"Según el último balance de criminalidad del Ministerio de Interior, desde enero hasta septiembre de 2022 se produjeron 217.571 ciberdelitos, lo que significa que en ese tiempo el 12,5% de los crímenes cometidos en nuestro país se llevaron a cabo de manera on-line. Y eso que por el momento no están incluidos los datos de cibercriminalidad de Ertzaintza y Mossos d' Esquadra, que estarán disponibles en el informe final anual. Así que, como avisa el propio Ministerio, "las cifras actuales reales serán superiores". Desde 2011 el número de delitos totales en España se ha mantenido bastante constante (en torno a los dos millones al año). Pero mientras la criminalidad convencional se ha ido reduciendo poco a poco, la cibercriminalidad no ha dejado de crecer a pasos agigantados." READ MORE

Latest reports

- Microsoft, MCCrash: Cross-platform DDoS botnet targets private Minecraft servers, 15 December 2022
- Meta, Meta Policy Recommendations for Tackling the Surveillance-for-Hire Industry, 15 December 2022
- OECD, Declaration on a Trusted, Sustainable and Inclusive Digital Future, 16 December 2022
- EPRS | European Parliamentary Research Service, EU cyber-resilience act, 17 December 2022
- Financesonline, 73 Important Cybercrime Statistics: 2022 Data Analysis & Projections, 20 December 2022
- Unit42, Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine, 20 December 2022
- ENISA, Cybersecurity Education Initiatives in the EU Member States, 20 December 2022
- Dice, Beyond Ransomware: Cybercrime Trends to Watch in 2023, 20 December 2022
- Group-IB, Godfather: A banking Trojan that is impossible to refuse, 21 December 2022
- Europol, SIRIUS Digital Evidence Situation Report 2022, 22 December 2022
- Astra, Cyber Crime Statistics 2023: Cost, Industries, and Trends, 23 December 2022
- Thales, What does 2023 have in store for cybercrime? Here are 16 predictions for a hacky new year, 27 December 2022
- Interpol, 2022: the year in review, 23 December 2022

Upcoming events

- 1-15 January 2023, C-PROC/LEBANON, (*on-line*), finalization of the basic judicial training course to be adopted by Lebanon, CyberSouth
- 6 January, C-PROC/NEPAL, *(hybrid),* Advisory mission on legislation, GLACY+
- 8-20 January, C-PROC, *(in-person),* Support the participation of delegates from a selected number of countries to the 4th meeting of the Ad Hoc Committee on new UN Treaty, GLACY+, CyberEast, CyberSouth, Octopus, iPROCEEDS-2
- 13 January, C-PROC, (*on-line)*, Second Webinar on raising awareness on the 1st Additional Protocol to the Budapest Convention, T-CY and 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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime