Cybercrime Digest

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

01 – 15 February 2022

Source: Council of Europe

Date: 09 Feb 2022

Save the date! International conference and opening for signature of the 2nd Additional Protocol to the Convention on Cybercrime

“Following almost four years of negotiations and formal approval on 17 November 2021, the 2nd Additional Protocol to the Budapest Convention on Cybercrime is now to be opened for signature by the Parties to the Convention at the Council of Europe in Strasbourg, France, on 12 May 2022, within the framework of an international conference on enhanced cooperation and disclosure of electronic evidence. The event will be held in cooperation with the Italian Presidency of the Committee of Ministers of the Council of Europe.” READ MORE

Source: Council of Europe

Date: 08 Feb 2022

Council of Europe celebrates Safer Internet Day 2022

“For the 7th consecutive year, the Council of Europe is supporting the Safer Internet Day Campaign and is joining forces with numerous stakeholders to work together for a better and safer internet for all, and especially for children and young adults. Safeguarding and promoting the rights of the child in the digital environment and keeping them safe online are at the heart of our work.” READ MORE

Source: European Commission

Date: 01 Feb 2022

Europol: Commission welcomes political agreement on stronger mandate

“The Commission welcomes today's political agreement between the European Parliament and the Council on a stronger mandate for Europol, the EU agency for law enforcement cooperation. […] Europol will be able to cooperate effectively with private parties. The updates also set clear rules on processing large and complex datasets, and allow the agency to develop new technologies that match law enforcement needs.” READ MORE

Source: Tech Xplore

Date: 03 Feb 2022

European oil port terminals hit by cyberattack

“Major oil terminals in some of Western Europe's biggest ports have fallen victim to a cyberattack at a time when energy prices are already soaring, sources confirmed on Thursday. Belgian prosecutors have launched an investigation into the hacking of oil facilities in the country's maritime entryways […]. In Germany, prosecutors said they were investigating a cyberattack targeting oil facilities in what was described as a possible ransomware strike, in which hackers demand money to reopen hijacked networks. […] The EU's Europol police agency said it was aware of the incidents in Germany and had offered support to authorities."At this stage the investigation is ongoing and in a sensitive stage," Europol spokeswoman Claire Georges said."” READ MORE

Source: US Department of Justice

Date: 08 Feb 2022

Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen

"Two individuals were arrested this morning in Manhattan for an alleged conspiracy to launder cryptocurrency that was stolen during the 2016 hack of Bitfinex, a virtual currency exchange, presently valued at approximately $4.5 billion. […] "IRS-CI Cyber Crimes Unit special agents have once again unravelled a sophisticated laundering technique, enabling them to trace, access and seize the stolen funds, which has amounted to the largest cryptocurrency seizure to date, valued at more than $3.6 billion."" READ MORE

RELATED ARTICLE:

Wired, CryptocurrencyThe DOJ's $3.6B Bitcoin Seizure Shows How Hard It Is to Launder Crypto, 9 Feb 2022

Source: Euroactiv

Date: 15 Feb 2022

Deal on EU tech rules possible by June, key lawmaker says

"European Union lawmakers and countries could reach a deal by the end of June on proposed tech rules forcing online platforms to better police the internet despite differences in their approach, the lawmaker steering the negotiations said on Monday (14 February). The Digital Services Act (DSA) proposed by EU antitrust chief Margrethe Vestager forces Amazon.com Inc, Apple Inc, Alphabet Inc unit Google and Facebook owner Meta to do more to tackle illegal content on their platforms or face fines up to 6% of global turnover." READ MORE

RELATED ARTICLE:

Brussels Morning, Tech giants welcome EU regulations against online hate — Brussels Morning Newspaper, 4 Feb 2022

Source: Politico

Date: 15 Feb 2022

Ukrainian Ministry of Defense websites hit by cyberattack

"The Ukrainian Ministry of Defense said in a tweet Tuesday that the websites were down, and that it was likely being targeted by a distributed denial of service, or DDoS, attack. A separate Ukrainian agency, the Centre for Strategic Communications and Information Security, said the website of the Armed Forces of Ukraine had also been attacked. The agency also said Ukrainian banks PrivatBank and Oschadbank had been targeted by the DDoS attack. The Ukrainian Cyberpolice said in a tweet that it had evidence that unidentified individuals were sending out text messages about fraudulent Ukrainian ATM failures." READ MORE

RELATED ARTICLES:

CNet, As Russia's cyberattacks on Ukraine mount, the risk of impact in other countries rises, 8 Feb 2022

The Conversation, Russia has been at war with Ukraine for years – in cyberspace, 7 Feb 2022

Source: WeLiveSecurity

Date: 10 Feb 2022

Hidden in plain sight: How the dark web is spilling onto social media

"Just a few years ago, illicit services and online contraband were firmly sourced in the hidden, largely untraceable depths of the internet: the dark web. People frequenting dark web sites knew how to take advantage of the anonymity offered, and often managed to evade law enforcement. […] In recent years, new platforms have emerged that criminals have co-opted, with perhaps Telegram being the most notable example. […] Unsurprisingly, however, the platform has also attracted the attention of criminals who are keen to take advantage of this privacy. On offer is everything from drugs, counterfeit money, stolen credit card details and other personal data to hitmen services (or, rather, hitman scams)." READ MORE

Source: 2021portugal.eu

Date: 10 Feb 2022

E-evidence Package: first trilogue meeting

"Under the Portuguese Presidency of the Council of the European Union, the trilogue today began negotiations with the Council, the European Parliament and the European Commission on the e-evidence legislative package, at a meeting chaired by the Assistant Secretary of State for Justice, Mário Belo Morgado Given the volatile nature and the transnational dimension of e-evidence, the aim is to provide the justice systems of the Member States with speedy judicial cooperation instruments that will assure the acquisition and preservation of evidence. This will help to effectively combat the criminal activity associated with the digitalisation of society, an activity which has intensified due to the conditions in place because of the current pandemic." READ MORE

Source: Council of Europe

Date: 10 Feb 2022

Information and communication technologies in elections: Council of Europe adopts new guidelines

"The Committee of Ministers has adopted a set of guidelines on the use of information and communication technologies (ICT) in the electoral process which aim at ensuring the integrity of the electoral process and therefore enhancing citizens' trust in democracy. Prepared by the European Committee on Democratic Governance (CDDG), the guidelines propose a set of requirements and safeguards to be introduced in the legislation and practices of Council of Europe member states when using ICT in the different stages of the electoral process." READ MORE

Source: Security Affairs

Date: 03 Feb 2022

Wormhole cryptocurrency platform hacked, crooks stole $326 million, the second-biggest hack of a DeFi platform

"Wormhole, one of the most popular bridges that links the Ethereum and Solana blockchains, lost about $325 million in an attack that took place on Wednesday. This is the second-biggest hack of a DeFi platform ever, just after the $600 million Poly Network security breach." READ MORE

RELATED ARTICLE:

Reuters, Jump Trading replaces stolen Wormhole funds after $320 mln crypto hack, 4 Feb 2022

Source: ENISA

Date: 08 Feb 2022

Cyber teams from across the globe to compete in 1st International Cybersecurity Challenge

"Building on the success of the so-called Capture-the-flag competitions (CTFs)'' ENISA, together with other regional and international organisations, decided to design and host for the first time the International Cybersecurity Challenge (ICC). With this first ever Cyber World Cup, which comprise a number of different cybersecurity challenges, we are entering a new dimension by moving up to a global scale with regional teams joining from all over the world." READ MORE

Source: Inews Guyana

Date: 09 Feb 2022

Guyana: Cybercrime Act: Sedition laws reintroduced by APNU/AFC will be removed at 'appropriate time'

"The sedition laws included in the controversial Cybercrime Act, which criminalises utterances against the Government of the day and which were introduced by the former A Partnership for National Unity/Alliance For Change (APNU/AFC) Government, will be reviewed and removed at the appropriate time. " READ MORE

Source: Pauta.ch

Date: 04 Feb 2022

Chile: ACTI: proyecto de ley de delitos informáticos "está yendo más allá" del Convenio de Budapest

"El Congreso está tramitando una ley que moderniza las normas sobre delitos informáticos que data de 1993. Sin embargo, hay una parte de ese proyecto que fue aprobada por la comisión mixta que está preocupando a diversos actores: la que estipula que el Ministerio Público podría pedir a los proveedores de servicio, sin orden judicial, información personal de sus abonados." READ MORE

Source: Council of Europe

Date: 08 Feb 2022

GLACY+ and Octopus Project: The Second Additional Protocol to the Budapest Convention – 2nd Webinar in the series for countries in Latin America

"On 8 February 2022, GLACY+ and the Octopus Project organised the second webinar from a series of four thematic webinars on the Introduction of the Second Additional Protocol to the Budapest Convention on enhanced cooperation and disclosure of electronic evidence." READ MORE

Source: Malwarebytes Labs

Date: 07 Feb 2022

Colombia and Peru: Securitas breached, 3TB of airport employee records exposed

"An unsecured AWS server, found open to the public Internet, is the root cause of a huge compromise of data of airport employees in Colombia and Peru. This server, according to a report, belongs to Securitas, a Stockholm-based multinational company that provides security services like security guarding, fire and safety, and supply-chain risk management among others. […] A compromised AWS server exposed sensitive company data, employee PII, and datasets of Securitas employees and airport employees." READ MORE

Source: Council of Europe

Date: 02 Feb 2022

CyberSouth: Third Working Group Meeting on the mainstreaming of judicial training material on cybercrime and electronic evidence in Jordan

"Under the framework of CyberSouth project, the third meeting on the mainstreaming of judicial training in Jordan took place online on the 1st of February 2022. The event was a follow-up to the second meeting of the working group focused on developing a manual on cybercrime and electronic evidence for Jordanian magistrates." READ MORE

Source: Council of Europe

Date: 08 Feb 2022

CyberSouth: National workshop on the preparation of criminal justice statistics on cybercrime and e-evidence in Lebanon

"A new series of national workshops, dedicated to the preparation of criminal justice statistics on cybercrime and e-evidence, was launched within the CyberSouth project, on the 8th of February 2022, with the organisation of the workshop for Lebanon." READ MORE

Source: Inquirer

Date: 09 Feb 2022

Philippines: Groups to gov't: Address gaps in imposing laws vs online child sexual abuse

"Groups on Wednesday called on the national government to address gaps in implementing existing laws against Online Sexual Abuse and Exploitation of Children (OSAEC). In a statement made after commemorating the annual Safer Internet Day held on Feb. 8, Atty. Tim Abejo, co-convenor of consumer group CitizenWatch, said that while laws have been created to curb online exploitation of children, gaps in implementation continue to allow OSAEC to thrive." READ MORE

Source: Threat Post

Date: 11 Feb 2022

India: Cybercrooks Frame Targets by Planting Fabricated Digital Evidence

"Threat actors are hijacking the devices of India's human rights lawyers, activists and defenders, planting incriminating evidence to set them up for arrest, researchers warn. The actor, dubbed ModifiedElephant, has been at it for at least 10 years, and it's still active. It's been shafting targets since 2012, if not sooner, going after hundreds of groups and individuals – some repeatedly – according to SentinelLabs researchers." READ MORE

Source: Philippines Information Agency

Date: 7 Feb 2022

Philippines to strengthen cybercrime policies against fraud

"As financial losses from fraud and scams continue to escalate, the Bankers Association of the Philippines (BAP) will continue to strengthen its partnership with the Department of Justice (DOJ) to generate action against cybercrimes." READ MORE

Source: Nikkei Asia

Date: 08 Feb 2022

North Korea targeted IAEA in cyberattacks draft U.N. report

“North Korea launched hacking attacks against the International Atomic Energy Agency as well as a key South Korean defense contractor, according to a draft United Nations report obtained by Nikkei on Monday. Kimsuky, a hacking group backed by North Korean intelligence authorities, is described as capable of staging phishing attacks that mimic well-known websites and software applications to trick victims into entering their credentials. "In one of the cases the actor collected email addresses of not only government entities but also of those associated with a security officer at the IAEA," the report says.” READ MORE

Source: Council of Europe

Date: 2-4 Feb 2022

CyberEast delivers a training course on Financial investigation, virtual currency and darknet for police and prosecutors in Georgia

“[…] The CyberEast project, a joint project of the European Union and the Council of Europe, has delivered a training course on Financial Investigation, Virtual Currency and Darknet for a group of 21 Georgian investigators and prosecutors on matters of cybercrime and financial investigations, during 2-4 February 2022, training which took place in Tsinandali, Georgia. This event has closed the series of similar training initiatives offered by the project in all of the region's countries (except Belarus)." READ MORE

Source: Front News

Date: 04 Feb 2022

New Council of Europe action plan for Ukraine - 2023-2026

“Representatives of the Council of Europe and the relevant public authorities of Ukraine discussed proposals for a new action plan of the Council of Europe for Ukraine in 2023-2026. This is reported by the UNN with reference to the portal of the Ministry of Foreign Affairs of Ukraine. The parties paid special attention to criminal justice reform, judicial reform, decentralization, the fight against cybercrime and ways to improve electoral processes in Ukraine.” READ MORE

Source: Krebs on Security

Date: 09 Feb 2022

Russian Govt. Continues Carding Shop Crackdown

“Russian authorities have arrested six men accused of operating some of the most active online bazaars for selling stolen payment card data. The crackdown — the second closure of major card fraud shops by Russian authorities in as many weeks — comes closely behind Russia’s arrest of 14 alleged affiliates of the REvil ransomware gang and has many in the cybercrime underground asking who might be next.” READ MORE

Source: Politico

Date: 15 Feb 2022

EU privacy watchdog urges ban on Pegasus

“The European Data Protection Supervisor has called for a ban on the spyware tool Pegasus to protect people's fundamental rights. Last July, an international investigation revealed that the spyware, developed by tech company NSO Group, could have been used by governments across the world, including in Poland and Hungary, to hack the phones of journalists, activists and politicians.” READ MORE

Source: Euractiv

Date: 08 Feb 2022

Europe is world's largest host of child pornography, advocacy groups say

""Europe is now the world's largest host of websites containing CSAM, which demands immediate action from EU member states," reads an open letter signed by 20 advocacy groups dedicated to child protection, including IWF, Thorn, Save the Children, 5Rights, and Eurochild. […] The NGOs point to the recent findings of Europol on child sexual exploitation, with more than 46 million unique images or videos of child abuse in its repository. In 2020, 86% of all known child sexual abuse material discovered online by the IWF was hosted in Europe." READ MORE

Source: Wired

Date: 03 Feb 2022

Germany has picked a fight with Telegram

"The country's new government is struggling to assert its authority over the messaging app, which officials believe has been used to organize violent incidents. […] German authorities believe Telegram has become the thread that ties together a series of violent incidents involving Germany's anti-lockdown movement. Shortly after the protest outside Köpping's home [N.B. Saxony's regional health minister, Petra Köpping], armed German police said they searched five properties linked to a Telegram group where members discussed plans to assassinate Saxony's prime minister, Michael Kretschmer, in retaliation for Covid restrictions." READ MORE

Source: ZD net

Date: 08 Feb 2022

Vodafone Portugal hit with cyberattack affecting 4G/5G network, TV, SMS services

"Vodafone Portugal announced on Tuesday that it was hit with a cyberattack that caused network disruptions across the country. "Vodafone was the target of a network disruption that began on the night of February 7, 2022, due to a deliberate and malicious cyberattack intended to cause damage and disruption. […]" the company said." READ MORE

Source: Bleeping Computer

Date: 10 Feb 2022

Spain dismantles SIM swapping group who emptied bank accounts

"Spanish National Police has arrested eight suspects allegedly part of a crime ring who drained bank accounts in a series of SIM swapping attacks. They presumably spoofed the targets' bank in phishing messages via email, SMS, or direct messages on social media platforms, according to a press release published today. By means of phishing, the suspects obtained the sensitive personal information needed to impersonate the potential victims and deceive phone store employees into issuing new SIM cards with the same number." READ MORE

Source: Bleeping Computer

Date: 11 Feb 2022

Croatian phone carrier data breach impacts 200,000 clients

"Croatian phone carrier 'A1 Hrvatska' has disclosed a data breach exposing the personal information of 10% of its customers, roughly 200,000 people. The announcement does not provide many details other than that they suffered a cybersecurity incident involving the unauthorized access of one of their user databases, which contained sensitive personal information. " READ MORE

Source: The Hacker News

Date: 10 Feb 2022

France rules that using google analytics violates GDPR data protection law

"French data protection regulators on Thursday found the use of Google Analytics a breach of the European Union's General Data Protection Regulation (GDPR) laws in the country, almost a month after a similar decision was reached in Austria. To that end, the National Commission on Informatics and Liberty (CNIL) ruled that the transatlantic movement of Google Analytics data to the U.S. is not "sufficiently regulated" citing a violation of Articles 44 et seq. of the data protection decree, which govern the transfers of personal data to third countries or international entities." READ MORE

Source: Info Security Magazine

Date: 07 Feb 2022

Swissport Ransomware attack delayed flights

"Airport services giant Swissport is restoring its IT systems after a ransomware attack struck late last week, delaying flights. "Due to system problems at our airport partner Swissport, 22 flights were delayed by three to 20 minutes yesterday," a spokeswoman for the airport is quoted as saying." READ MORE

Source: TV Europa

Date: 09 Feb 2022

Ciberataques com Emotet atingem 11% das organizações portuguesas

"Em Portugal 11% das empresas são vítimas de ciberataques com malware Emotet. Este malware evasivo é difícil de detetar, e utiliza múltiplos métodos para infetar redes. Investigadores da Check Point alertam que a Saúde é o setor atualmente mais atacado em Portugal. Investigadores de segurança da empresa de soluções de cibersegurança, Check Point, alertam para o regresso do Emotet ao primeiro lugar da lista mundial, com o Trickbot "destronado" após um longo período na posição cimeira." READ MORE

Source: Reuters

Date: 09 Feb 2022

European, U.S. regulators tell banks to prepare for Russian cyberattack threat

"The European Central Bank is preparing banks for a possible Russian-sponsored cyber-attack as tensions with Ukraine mount, two people with knowledge of the matter said, as the region braces for the financial fallout of any conflict. […] Its concerns are mirrored around the world. The New York Department of Financial Services issued an alert to financial institutions in late January, warning of retaliatory cyber-attacks should Russia invade Ukraine and trigger U.S. sanctions, according to Thomson Reuters' Regulatory Intelligence." READ MORE

Source: ZD Net

Date: 09 Feb 2022

FBI warns: SIM-swapping attacks are rocketing, don't brag about your crypto online

"The Federal Bureau of Investigation (FBI) is warning about a big uptick in scams using smartphone SIM swapping to defraud victims. Subscriber Identity Module (SIM) swapping is an old trick, but the FBI has issued a new alert about it because of a massive leap in reported cases in 2021 compared to previous years. […] Complaints to the FBI's Internet Crime Complaint Center (IC3) have skyrocketed in the past year." READ MORE

Source: Associated Press

Date: 2 Feb 2022

US: Hackers prey on public schools, adding stress amid pandemic

"Cyberattacks like the one that cancelled classes for two days in Albuquerque's biggest school district have become a growing threat to U.S. schools, with several high-profile incidents reported since last year. And the coronavirus pandemic has compounded their effects: More money has been demanded, and more schools have had to shut down as they scramble to recover data or even manually wipe all laptops." READ MORE

Latest reports

- Cloudwards, Top Cyber Security Statistics, Facts & Trends in 2022, 1 February 2022
- Orange, Security Navigator 2022, 2 February 2022
- Lowy Institute, Big Data and National Security: A Guide for Australian Policymakers, 2 February 2022
- Digital Europe, Final steps towards a targeted and predictable Digital Markets Act, 2 February 2022
- 20 minutes, Cybercriminalité: Pourquoi la fraude à l'identité est-elle en constante augmentation?, 2 February 2022
- Stormshield.com, What are the cybersecurity trends for 2022?, 2 February 2022
- UK Parliament - Economic crime Report, 2 February 2022
- Trip Wire, Privacy in 2021: A Year Worth Reviewing | The State of Security, 3 February 2022
- Krebs on Security, How Phishers Are Slinking Their Links Into LinkedIn, 3 February 2022
- International Institute for Strategic Studies, Assessing military cyber maturity: strategy, institutions and capability, 3 February 2022
- Security Brief, Tackling the evolving threat of ransomware in 2022, 3 February 2022
- FBI, Indicators of Compromise Associated with LockBit 2.0 Ransomware, 4 February 2022
- Cabinet Office UK, National Cyber Strategy 2022, 7 February 2022
- Pew Research Center, Visions of the Internet in 2035, 7 February 2022
- HackRead, How Your Smartphone Can Be Used to Steal Your Data, 8 February 2022
- Intel471, PrivateLoader: The first step in many malware schemes, 8 February 2022
- UNICEF, Philippines sees increase in cyber tip reports in 2021; UNICEF calls for collective action on Safer Internet Day, 9 February 2022
- Digital Shadow, Valentine's Day: Share your love, not your credentials, 9 February 2022
- EDRI, Chat control: 10 principles to defend children in the digital age, 9 February 2022
- Cybersecurity & Infrastructure Security Agency, 2021 Trends Show Increased Globalized Threat of Ransomware, 9 February 2022
- ZD Net, Linux malware attacks are on the rise, and businesses aren't ready for it, 10 February 2022
- Bleeping Computer, FTC says Americans lost $547 million to romance scams in 2021, 10 February 2022
- Malwarebytes Labs, The world's most coveted spyware, Pegasus: Lock and Code S03E04, 14 February 2022
- Risk Based Security, 2021 Year End Report Vulnerability QuickView, February 2022

Upcoming events

- 16 February, C-PROC/VANUATU, (*online*), Advisory Mission on data protection legislation, GLACY+
- 16 February, C-PROC/NORTH MACEDONIA, (*online*), Domestic workshop on cybercrime and cybersecurity trends as well as for criminal justice statistics, iPROCEEDS-2

- 16 February, C-PROC/NORTH MACEDONIA, (*online*), Reports on cybercrime and cybersecurity trends as well as for criminal justice statistics, iPROCEEDS-2
- 17 February, C-PROC/JORDAN, (*online*) National Workshop on the development of criminal justice statistics on cybercrime and e-evidence, CyberSouth
- 21 February, C-PROC/INTERPOL, (*online*), Cryptocurrency and Dark Web Investigations Online – eCDWI, GLACY+, iPROCEEDS-2
- 21 February, C-PROC/PHILIPPINES, (*online*), Second Workshop on COVID-19 related cybercrime and e-evidence, OCTOPUS,
- 22 February, C-PROC/THE GAMBIA, (*online*), Support on the data protection bill, GLACY+
- 22 February, C-PROC/ALGERIA, (*online*) National Workshop on the development of criminal justice statistics on cybercrime and e-evidence, CyberSouth
- 22-24 February, C-PROC/SERBIA, MONTENEGRO AND BOSNIA AND HERZEGOVINA, (*online*), Training Course on Financial Investigations, Virtual Currencies and Darknet, iPROCEEDS-2
- 23 February, C-PROC/MOROCCO, (*online*), National Workshop on the development of criminal justice statistics on cybercrime and e-evidence, CyberSouth
- 24 February, C-PROC/LATAM, (*online*), Series of webinars on the Second Additional Protocol to the Budapest Convention for LATAM and Caribbean countries, GLACY+, OCTOPUS
- 24-25 February, C-PROC/TURKEY, (*in-person*), Support cooperation forums of cybercrime and cybersecurity experts (with CybersecurityEAST) – Practical use cases for SOPs, CyberEast
- 28 February-11 March, C-PROC, (*hybrid*), Participation in the UN ADHOC meeting on the new treaty on cybercrime, OCTOPUS
- 28 February, C-PROC/LEBANON, (*online*), National Workshop on the development of a domestic toolkit for first responders to cybercrime investigations, CyberSouth
- February-March, C-PROC, (*desk research*), Guidelines on the prevention and control of online fraud and criminal money flows, CyberEast
- February-May, C-PROC, (*online*), Translation of Second Additional Protocol to the Budapest Convention to support legal reforms and accession process, CyberEast

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of February have been rescheduled to a later date.

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