Cybercrime Digest

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

16 – 30 April 2022

Source: Joint Brussels Office

Date: 22 April 2022

The Council of the EU authorises member states to sign international agreement on e-evidence

"On 5 April, the Council of the EU adopted a decision authorising member states to sign, in the interests of the EU, the second additional protocol to the Convention on Cybercrime of the Council of Europe (the Budapest Convention). The protocol aims to improve cross-border access to electronic evidence co-operation between member states and third countries, while ensuring a high level of protection for individuals and the compliance with EU data protection standards." READ MORE

Source: EUROJUST

Date: 21 April 2022

Takedown of infrastructure of call centres involved in online investment fraud responsible for losses of at least EUR 20 million

"At the request of the Estonian authorities, Eurojust and Europol have assisted the takedown of an online investment fraud scheme, which defrauded victims of at least EUR 20 million. Authorities in Finland, the Netherlands, Latvia, France, Germany and Ukraine supported the operation, taking place today, during which more than fifty servers and services were seized in six countries. […] In addition to the fraudulent offers, the perpetrators installed remote access programmes that allowed them to illegally access the victims' computers and steal their banking credentials (bank card data, cryptocurrency wallet access information)." READ MORE

Source: Microsoft

Date: 27 April 2022

The hybrid war in Ukraine

"Starting just before the invasion, we have seen at least six separate Russia-aligned nation-state actors launch more than 237 operations against Ukraine – including destructive attacks that are ongoing and threaten civilian welfare. The destructive attacks have also been accompanied by broad espionage and intelligence activities. The attacks have not only degraded the systems of institutions in Ukraine but have also sought to disrupt people's access to reliable information and critical life services on which civilians depend and have attempted to shake confidence in the country's leadership." READ MORE

RELATED REPORT:

Microsoft, An overview of Russia's cyberattack activity in Ukraine

RELATED ARTICLES:

Ukrainian CERT, Cyberattack on state organizations of Ukraine using the malicious program IcedID, 14 April 2022 (updated 18 April 2022)

Symantec Enterprise Blogs, Shuckworm: Espionage Group Continues Intense Campaign Against Ukraine, 20 April 2022

Source: INTERPOL

Date: 26 April 2022

Illegal webtoon site shut down as part of joint collaboration

"Joint collaboration between INTERPOL, Korean and Moroccan law enforcement resulted in the shutdown of an illegal webtoon site and detention of a suspect. Moroccan authorities facilitated this action, thereby dismantling the criminal enterprise and protecting the rights of copyright holders. […] The successful collaboration comes under the INTERPOL Stop Online Piracy Project (I-SOP). […] By working in collaboration with member countries and private and public bodies, I-SOP aims to combat crimes involving intellectual property infringement such as trademark counterfeiting and copyright piracy." READ MORE

Source: The White House

Date: 28 April 2022

FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet

"Today, the United States with 60 partners from around the globe launched the Declaration for the Future of the Internet. […] This Declaration represents a political commitment among Declaration partners to advance a positive vision for the Internet and digital technologies. It reclaims the promise of the Internet in the face of the global opportunities and challenges presented by the 21st century. It also reaffirms and recommits its partners to a single global Internet – one that is truly open and fosters competition, privacy, and respect for human rights." READ MORE

RELATED DECLARATION:

The White House, Declaration for the Future of the Internet, 28 April 2022

Source: INTERPOL

Date: 26 April 2022

Global cooperation vital to ensuring better protection of intellectual property rights

"Intellectual property (IP) rights play a vital role in protecting innovation and supporting competitiveness. With adequate IP protection and support, young innovators can mobilize and help advance developments in the fields of business and science to improve health outcomes. In this context, the theme of this year's World IP Day is 'IP and Youth: Innovating for a better future'." READ MORE

Source: Hogan Lovells

Date: 25 April 2022

Cyber Resilience Act - New initiative to create cybersecurity rules for digital products

"In a call for Evidence for an Impact Assessment, the European Commission has introduced its initiative for a new Cyber Resilience Act that is set to establish new cybersecurity rules for digital products and ancillary services. The initiative aims to tackle practical challenges and potential gaps of the current legislation by introducing new man objectives the initiative plans to implement. Until the general public has the chance make itself heard as part of the consultation process." READ MORE

Source: Republique du Cameron

Date: 27 April 2022

Loi N°2022/002 du 27 avril 2022 autorisant le Président de la République à procéder à l'adhésion du Cameroun à la Convention de Budapest sur la cybercriminalité

"Le Président de la République est autorisé à procéder à l'adhésion du Cameroun à la Convention de Budapest sur la cybercriminalité, adoptée le 23 novembre 2001 à Budapest (Hongrie)." READ MORE

Source: Council of Europe

Date: 28 April 2022

GLACY+ and APWG: webinar explores international cooperation on cybercrime using emerging technologies

"On 28 April, the Global Action on Cybercrime Extended (GLACY+) project and the Anti-phishing Working Group (APWG) held a roundtable discussion on international cooperation to prevent, investigate and prosecute cybercrime using emerging technologies. The conversation focused on the challenges and opportunities in this field." READ MORE

Source: KrebsOnSecurity

Date: 22 April 2022

Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code

"KrebsOnSecurity recently reviewed a copy of the private chat messages between members of the LAPSUS$ cybercrime group in the week leading up to the arrest of its most active members last month. The logs show LAPSUS$ breached T-Mobile multiple times in March, stealing source code for a range of company projects. T-Mobile says no customer or government information was stolen in the intrusion. LAPSUS$ is known for stealing data and then demanding a ransom not to publish or sell it. […] From its inception in December 2021 until its implosion late last month, LAPSUS$ operated openly on its Telegram chat channel, which quickly grew to more than 40,000 followers after the group started using it to leak huge volumes of sensitive data stolen from victim corporations." READ MORE

RELATED ARTICLE:

Security Week, Lapsus$ Hackers Gained Access to T-Mobile Systems, Source Code, 25 April 2022

Source: Council of Europe

Date: 14 April 2022

The International Network of National Judicial Trainers: third P2P workshop (second series)

"Within the framework of the second series of practitioners-to-practitioners workshops of the International Network of National Judicial Trainers, a third webinar was held on 14 April focusing on Online child sexual exploitation abuse (OCSEA). Five national judicial trainers from Tunisia, Brazil, Dominican Republic and Tonga, presented their countries' approach and legislation on this matter, as well as investigation techniques." READ MORE

Source: Bloomberg

Date: 26 April 2022

Tech Giants Duped Into Giving Up Data Used to Sexually Extort Minors

"Major technology companies have been duped into providing sensitive personal information about their customers in response to fraudulent legal requests, and the data has been used to harass and even sexually extort minors, according to four federal law enforcement officials and two industry investigators. […] The tactic is considered by law enforcement and other investigators to be the newest criminal tool to obtain personally identifiable information that can be used not only for financial gain but to extort and harass innocent victims." READ MORE

Source: Central America

Date: 19 April 2022

Costa Rica Cyber Attack Currently Underway

"The Costa Rica Finance Ministry website is still down this morning, after it emerged yesterday that the Conti ransomware group – a Russian "hacking-by-hire" collective – had breached its security and stolen a terabyte of data containing taxpayer info. Conti has encrypted this data and has threatened to release it on April 23rd unless they receive a US$10 million ransom payment. […] Later on yesterday evening, MICITT (the Costa Rican Ministry of Science & Technology) also confirmed a breach in their website. As it stands this morning, their site is also still down. […] The government has also said it has no intention of paying any ransom to the hackers." READ MORE

Source: SWI

Date: 25 April 2022

Colombia, España y el Consejo de Europa colaboran contra delitos cibernéticos

"Colombia, España y el Consejo de Europa colaboran en la lucha contra la delincuencia cibernética, con el fin de avanzar en el combate contra el uso de tecnologías de la información con fines delictivos, informó este lunes la embajada colombiana en Madrid. Con este objetivo, entre los próximos 27 a 29 de abril la Embajada de Colombia en Madrid, el Consejo de Europa y el Ministerio de Justicia de España tienen previsto en Bogotá un taller sobre ciberdelincuencia, centrado en contenidos como el Convenio de Budapest, el primer tratado internacional contra delitos a través de internet, en vigor desde 2004." READ MORE

Source: 24 Heures au Benin

Date: 21 April 2022

Comment muscler la cybersécurité de la finance africaine ?

"L'Afrique rattrape son retard numérique rapidement. Par corollaire, la constante hausse de la pénétration de l'internet s'accompagne, mécaniquement, de l'augmentation de la cybercriminalité. Une réalité qui touche particulièrement les banques et les fintechs du continent. On estime à près de 3000 le nombre d'institutions bancaires vulnérables aux cyber menaces (selon la Banque africaine de développement) et à 250 millions le nombre de clients exposés. De facto, le continent est très mal protégé dans le cyberespace, et plus particulièrement la sphère financière, parmi les plus attaquées." READ MORE

Source: Zawya

Date: 28 April 2022

Data security and privacy laws develop across Africa

"Numerous countries in Africa have developed or implemented data privacy and security laws in their countries in the last few years. With the rapid rise in digitisation as a result of the pandemic, the broad implementation of such laws across the continent has never been more urgent. Countries including Ghana, Kenya, Madagascar, Mauritius, Nigeria, Rwanda, South Africa, Togo, Uganda and Zimbabwe have been implementing new measures to protect and secure the personal information of their citizens." READ MORE

Source: News Ghana

Date: 20 April 2022

Gambia, Sierra Leone and Mozambique seek support from Cyber Security Authority

"Three African countries, The Gambia, Sierra Leone and Mozambique, have called on the Cyber Security Authority (CSA) for collaboration and support for the development of cybersecurity in their countries. Within the last five years, Ghana has taken progressive steps towards the development of cybersecurity in the country." READ MORE

Source: Council of Europe

Date: 27 April 2022

The GLACY+: Support for data protection legislation in Vanuatu – Workshop for drafting the Data Protection and Privacy Policy

"Organised in the framework of the Global Action on Cybercrime Extended (GLACY+) project, together with the Council of Europe's Data Protection Unit, the third workshop to support the drafting of data protection legislation in Vanuatu took place on 27 April 2022. It provided an opportunity for members of the Vanuatuan national expert task force to discuss the draft Data Protection and Privacy Policy of Vanuatu, prepared with support from the Council of Europe." READ MORE

Source: Just Security

Date: 20 April 2022

To Support Accountability for Atrocities, Fix U.S. Law on the Sharing of Digital Evidence

"International justice mechanisms will insist upon unassailable evidence of the alleged atrocities. However, a vast amount of potential evidence in the form of photos and videos uploaded by Ukrainians on social media platforms is at risk or potentially unavailable to courts. The risk arises from the loss of evidence due to the permanent removal of content deemed to have violated platforms' terms of service." READ MORE

Source: Dutch News

Date: 28 April 2022

Police arrest 10 men from same family in underground banking probe

"Amsterdam police have arrested 10 men from the same family after a two-year investigation into money laundering on a massive scale, involving both cash and crypto currencies. […]On the day of raids, involving over 200 people and 15 locations, officials seized €1.4 million in cash, plus bitcoin, a gun, luxury items, phones and computers." READ MORE

Source: EURACTIV

Date: 27 April 2022

EU's cyber incident reporting mechanism does not work, agency chief warns

"The head of the EU's flagship cybersecurity agency has warned that its incident reporting system is too bureaucratic and "does not work", and called for a more resilient system, as well as a better legislative environment and information sharing with member states. […] An update of the EU Directive on Security of Network and Information Systems (NIS), which should address these shortcomings, is currently being negotiated." READ MORE

Source: Bank Info Security

Date:22 April 2022

Pro-Russian Killnet Group in DDoS Attacks on Czech Entities

"Pro-Russia threat group Killnet has attacked several entities in recent days. It targets victims that it believes are adversaries of Russia in the Russia-Ukraine war. This specifically includes NATO and its allied members. According to a post viewed by Information Security Media Group in the group's Telegram channel, Killnet, the group says that it does not wish to harm the people of other countries and it does not provide any hacking services to others. It says "the task of killnet is to create maximum damage to the network info structure of enemy countries." READ MORE

RELATED ARTICLE:

Expats CZ, Czech Television hit in another wave of cyber-attacks, 29 April 2022

Source: BNT News

Date: 18 April 2022

Cyber-attack on Bulgarian Posts disrupts payment of pensions

"A cyber-attack on the computer systems of "Bulgarian Posts" caused disruptions with the payment of pensions and Easter allowances. In the morning on April 18, the Bulgarian Posts assured that there would be no interruption in the payment of the money. In Plovdiv and Rousse, however, many pensioners could not receive their pensions and allowances. The hacker attack was detected on Saturday, April 16 and measures were immediately taken to transfer the Bulgarian Posts system to the state cloud infrastructure. An assessment is being made as to how far the system has been affected by the malicious cyber attack." READ MORE

Source: Security Affairs

Date: 27 April 2022

Wind Turbine giant Deutsche Windtechnik hit by a professional Cyberattack

"German wind turbine giant Deutsche Windtechnik announced that some of its systems were hit by a targeted professional cyberattack earlier this month. […] Deutsche Windtechnik did not disclose details about the attack, but experts believe that the company was hit with ransomware. At the end of March, the Conti ransomware gang hit the manufacturer of wind turbines Nordex, while in early March, wind turbine manufacturer Enercon GmbH lost remote connection to roughly 5,800 turbines due to an attack on Viasat's satellite network." READ MORE

Source: Times Now

Date: 30 April 2022

DDos cyberattack by pro-Russian cyber gang Killnet hit Romanian websites

"Romanian government on Friday claimed cyberattacks on websites of public institutions, including the Defence Ministry. Romania's cybersecurity agency said that the pro-Russia cybercrime group attacked the government websites over its support to Ukraine against Russia's invasion. Romania's National Cybersecurity Agency in a statement said that A series of attacks hit "public institutions and private entities". The agency claimed that the official websites of the border police, defence ministry and railways were affected by the DDoS attack." READ MORE

Source: The Guardian

Date: 20 April 2022

Apple to roll out child safety feature that scans messages for nudity to UK iPhones

"A safety feature that uses AI technology to scan messages sent to and from children will soon hit British iPhones, Apple has announced. The feature, referred to as "communication safety in Messages", allows parents to turn on warnings for their children's iPhones. When enabled, all photos sent or received by the child using the Messages app will be scanned for nudity. […] The company is also introducing a set of features intended to intervene when content related to child exploitation is searched for in Spotlight, Siri or Safari." READ MORE

Latest reports

- CyberScoop, Prolific cyber extortion group Karakurt might be a Conti side hustle, 15 April 2022
- Time, How Ukraine Is Crowdsourcing Digital Evidence of War Crimes, 18 April 2022
- Bleeping Computer, LinkedIn brand takes lead as most impersonated in phishing attacks, 19 April 2022
- Joint Cybersecurity Advisory of the cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, 20 April 2022
- Bleeping Computer, Microsoft Exchange servers hacked to deploy Hive ransomware, 20 April 2022
- Wired, Hackers Are Getting Caught Exploiting New Bugs More Than Ever, 21 April 2022
- Trend Micro, Cybersecurity Predictions for 2022, 24 April 2022
- Journal de Cybersecurity, Accessible from the open web: a qualitative analysis of the available open-source information involving cyber security and critical infrastructure, 26 April 2022
- Help Net Security, Meteoric attack deploys Quantum ransomware in mere hours, 26 April 2022
- Microsoft, An overview of Russia's cyberattack activity in Ukraine, 27 April 2022
- Europol, Facing reality? Law enforcement and the challenge of deepfakes, 28 April 2022
- Cuestiones Politicas, The use of electronic evidence in court: a comparative legal analysis in the world practice, 28 April 2022
- Secure List by Kaspersky, APT trends report Q1 2022, 27 April 2022
- The New Statesman Spotlight, Cyber Security: The global threat landscape, 29 April 2022
- CERT New Zealand, Quarter Four Report 2021, April 2022
- Seek Research Magazine, Researchers tackle the new world of cybersecurity, Spring 2022

Upcoming events

- 3-4 May, C-PROC, *(online),* International law enforcement training course on investigating ransomware attacks, GLACY+, CyberSouth, CyberEast, iPROCEEDS-2
- 9 May-17 June, C-PROC, *(online),* Fundamentals of Open Source Investigation (FOSI) Training course, GLACY+
- 10-13 May, C-PROC/FRANCE, *(in-presence),* T-CY Plenary and International Conference & opening for signature of the Second Additional Protocol to the Convention on Cybercrime, T-CY, GLACY+, CyberSouth, CyberEast, OCTOPUS, iPROCEEDS-2
- 11-13 May, C-PROC/TURKEY, *(in-presence),* Training Course on Financial Investigations, Virtual Currencies and Darknet, iPROCEEDS-2
- May, C-PROC/ARMENIA, *(online),* Expert review of the new Code of Criminal Procedure - compliance with the Convention, CyberEast
- May-June, C-PROC/EAP countries, *(online),* Review of 2017 Report on Public–Private Cooperation - Development of guidelines for effective access to data, CyberEast

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