Cybercrime Digest

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

15 – 31 January 2023

Source: Council of Europe

Date: 24 Jan 2023

Greece becomes 31st State to sign the Second Additional Protocol to the Convention on Cybercrime

"The Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence was opened for signature on 12 May 2022 within the framework of an international conference in Strasbourg, France. Last Friday, on 20 January 2023, Ambassador Panayiotis Beglitis, Permanent Representative of Greece, signed the Protocol in presence of Council of Europe Secretary General Marija Pejčinović Burić, bringing the number of signatories up to 31." READ MORE

Source: Council of Europe

Date: 27 Jan 2023

France and Germany become 32nd and 33rd States to sign the Second Additional Protocol to the Convention on Cybercrime

"The Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence was opened for signature on 12 May 2022 within the framework of an international conference in Strasbourg, France. This morning, on 27 January 2023, Ambassador Marie FONTANEL, Permanent Representative of France, and Ambassador Jutta FRASCH, Permanent Representative of Germany, signed the Protocol in presence of the Deputy Secretary General Mr Bjorn BERGE, bringing the number of signatories up to 33." READ MORE

Source: Council of Europe

Date: 30 Jan 2023

Iceland joins the First Additional Protocol to the Convention on Cybercrime, on countering xenophobic and racist acts committed through computer systems

"On Monday, 30 January 2023, the Icelandic Ambassador to the Council of Europe, Ms Ragnhildur Arnljótsdóttir, deposited the instrument of ratification of the First Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)." READ MORE

Source: Council of Europe

Date: 30 Jan 2023

Dominican Republic becomes the 34th State to sign the Second Additional Protocol to the Convention on Cybercrime

"On Monday, 30 January 2023, the Ambassador of the Dominican Republic to the Kingdom of Belgium and the European Union, Mr Iván Ogando Lora, signed the Second Additional Protocol to the Convention on Cybercrime […]. The event took place in Strasbourg in the presence of the Deputy Secretary General of the Council of Europe, Mr Björn Berge, and the Ambassador for Cyber Matters at the Ministry of Foreign Affairs of the Dominican Republic, Mr Claudio Peguero." READ MORE

Source: Eucrim

Date: 26 Jan 2023

Green Light for Ratification of CoE's E-Evidence Treaty

"The European Parliament gave green light for EU Member States to ratify the Second Additional Protocol to the Convention on Cybercrime. The Additional Protocol builds on the 2001 Budapest Convention on Cybercrime and regulates the cross-border exchange of electronic evidence in criminal proceedings. On 17 January 2023, the European Parliament decided to give its consent to the draft Council Decision. […] After the EP's consent (as required by Art. 218(6) TFEU), the Council can now adopt the act. Since the EU cannot become a party to the Protocol, the Council's decision will enable Member States to act jointly in the interest of the EU and ratify the CoE treaty." READ MORE

RELATED ARTICLE:

Council of the European Union, Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence, 25 Jan 2023

Agence Europe, European Parliament approves ratification of second protocol to Budapest Convention on Cybercrime, 17 January 2023

Source: Euronews

Date: 24 Jan 2023

Ukraine blames Russia for most of over 2,000 cyberattacks in 2022

"KYIV – A senior Ukrainian official blamed Russia on Tuesday for carrying out the bulk of more than 2,000 cyberattacks on Ukraine in 2022, speaking at a news conference that he said was itself delayed because of a cyberattack. The official, Yuriy Schygol, told reporters that his livestreamed conference was forced to start 15 minutes late because of a Russian hack, though he did not elaborate or present evidence for his assertion. […] During the news briefing, he said Ukraine had been hit by 2,194 cyberattacks in 2022, with 1,655 of those coming after Moscow's Feb. 24 invasion." READ MORE

RELATED ARTICLE:

Tech Digi Pro, Ukraine Hit with new golang-based ''SwiftSlicer '' Malware in latest cyberattack, 28 Jan 2023

Source : EUROPOL

Date :26 Jan 2023

Cybercriminals stung as HIVE infrastructure shut down

"Europol supported the German, Dutch and US authorities in taking down the infrastructure of the prolific HIVE ransomware. This international operation involved authorities from 13 countries in total. […] In the last year, HIVE ransomware has been identified as a major threat as it has been used to compromise and encrypt the data and computer systems of large IT and oil multinationals in the EU and the USA. Since June 2021, over 1 500 companies from over 80 countries worldwide have fallen victim to HIVE associates and lost almost EUR 100 million in ransom payments." READ MORE

RELATED ARTICLE:

Washington Post, FBI shuts down ransomware gang that targeted schools and hospitals, 26 Jan 2023

Source: The Record

Date:17 Jan 2023

China proposes UN treaty criminalizes 'dissemination of false information'

''China has proposed that a new international convention on cybercrime should criminalize the "dissemination of false information" during negotiations in Vienna about the provisions of the United Nations treaty. The proposal is likely to be contested by Western states who will see it as a threat to human rights standards and an attempt by the Chinese Communist Party to legitimize its controls, and those of like-minded governments, over what people can see and share online. […] Last week, during the ongoing negotiations regarding the specifics of the new treaty, the provisions that had been put forward were separated into two categories – those with broad support and those which were more contested.'' READ MORE

Source: Council of Europe

Date:30-31 Jan 2023

Octopus Project: International Conference on xenophobia and racism committed through computer systems - sharing good practices on 20 years of implementing the First Additional Protocol to the Convention on Cybercrime

"Some 110 experts on cybercrime and hate speech from over 45 countries – including from public and private sectors, academia and civil society organisations – participated in the International Conference on xenophobia and racism committed through computer systems at the Council of Europe in Strasbourg, France, and online from 30 to 31 January 2023. The conference was held on the occasion of the 20th Anniversary of the first "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189)".'' READ MORE

Source: Europol

Date: 23 Jan 2023

Bitzlato: senior management arrested

"An operation led by French and US authorities, and strongly supported by Europol, has targeted the crypto exchange platform Bitzlato. The globally operating Hong Kong-registered cryptocurrency exchange is suspected of facilitating the laundering of large amounts of criminal proceeds and converting them into roubles. […] The operation also involved law enforcement and judicial authorities from Belgium, Cyprus, Portugal, Spain and the Netherlands. […] While the conversions of crypto-assets into fiat currencies is not illegal, investigations into the cybercriminal operators indicated that large volumes of criminal assets were going through the platform. The analysis indicated that about 46 % of the assets exchanged through Bitzlato, worth roughly EUR 1 billion, had links to criminal activities." READ MORE

RELATED ARTICLE:

US Department of Justice, Founder and Majority Owner of Cryptocurrency Exchange Charged with Processing Over $700 Million of Illicit Funds, 18 January 2023

Source: ENISA

Date: 27 Jan 2023

Protecting Data: Can we Engineer Data Sharing?

"To celebrate the European Data Protection Day on 28 January 2023, ENISA publishes today its report on how cybersecurity technologies and techniques can support the implementation of the General Data Protection Regulation (GDPR) principles when sharing personal data. […] The EU Agency for Cybersecurity has been working in the area of privacy and data protection since 2014, by analysing technical solutions for the implementation of the GDPR, privacy by design and security of personal data processing. […] This work builds upon the Agency's activities in the area of Data Protection Engineering and is produced in collaboration with the ENISA Ad Hoc Working Group on Data Protection Engineering." READ MORE

Source: Security Week

Date: 19 Jan 2023

Attacks and cyberattacks on satellites becoming more common, says EU's top diplomat

"Attacks and cyberattacks on satellites are becoming more common and a cause for security concerns, according to the EU's foreign affairs chief. Josep Borrell said on Tuesday that one of those attacks was a clear sign of the start of the Russian invasion of Ukraine. Speaking at the opening of the European Space Conference in Brussels, the EU's High Representative for Foreign Affairs said that 24 hours before Moscow invaded its neighbour in February last year, the space telecommunication network used by the Ukrainian army was targeted by a cyberattack and that the malicious code used managed to bring down parts of the network. There are now 5,500 satellites in orbit, with around 10% used by the world's military. NATO is now defining space as one of the most important areas. But Borrell said risks could also come from the physical destruction of satellites." READ MORE

Source: Tech Crunch

Date: 24 Jan 2023

FBI accuses North Korean government hackers of stealing $100M in Harmony bridge theft

"The FBI accused two groups of North Korean government hackers of carrying out last year's heist of $100 million in crypto stolen from a company that allows users to transfer cryptocurrency from one blockchain to another. On Monday, the FBI announced that the Lazarus Group and APT38 — two groups linked to the North Korean government by both cybersecurity companies and government agencies — were responsible for the hack against the Horizon bridge, created by the U.S. company Harmony, in June 2022." READ MORE

Source: Security Week

Date: 19 Jan 2023

Meta Slapped With 5.5 Million Euro Fine for EU Data Breach

"Social media giant Meta has been fined an additional 5.5 million euros ($5.9 million) for violating EU data protection regulations with its instant messaging platform WhatsApp, Ireland's regulator announced Thursday. The penalty follows a far larger 390-million-euro fine for Meta's Instagram and Facebook platforms two weeks ago after they were found to have flouted the same EU rules. In its new decision, the Irish Data Protection Commission (DPC) found the group acted "in breach of its obligations in relation to transparency," the watchdog said in a statement." READ MORE

Source: Security week

Date: 27 Jan 2023

Inside the Rising Cybercrime Threat in Latin America

"A cyber intelligence firm was asked by a Columbian bank customer to investigate the persistent phishing campaigns it had been experiencing. This triggered a wider examination of cybercrime across the whole Latin America region — and discovered a melting pot (described as a 'perfect storm') of social, geopolitical and economic conditions promoting a dramatic rise in cybercriminal activity. There are several triggers. Firstly, economic problems locally centered on Venezuela but affecting the whole region and exacerbated by global trade conditions are causing genuine hardship throughout the region for many young people. Some of these people are turning to cybercrime as a means — if not the only means — of earning money. Secondly, there is a high use of the internet among a huge population with a low awareness of cyber security awareness." READ MORE

Source: Jurist.org

Date: 20 Jan 2023

Uganda Constitutional Court declares controversial section of communications law void

"The Ugandan Constitutional Court Tuesday declared a section of the Computer Misuse Act, No. 2 of 2011 void with enforcement banned. Section 25 of the act prohibited any person from "willfully and repeatedly [using] electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication." The petitioners claimed section 25 was overly vague and limited free speech. […] The Ugandan government is facing numerous lawsuits brought by journalists and civil action groups. […] The current lawsuits again cite intentional vagueness with alleged political motivations." READ MORE

Source: All Africa

Date: 17 Jan 2023

South Africa: Leading Law Firm Ordered to Pay Victim of Cyber Crime

"One of South Africa's leading law firms has been held liable for R5.5 million which a property buyer intended to deposit in its trust account. The money was stolen as a result of fraudsters manipulating emails from an employee of the firm. […] In her arguments, Hawarden claimed that ENS owed her a duty of care, and that in corresponding with her, it also had a legal duty to warn her of the danger of "business email compromise (BEC)", that this was on the increase and that it was already prevalent." READ MORE

Source: IT Web

Date:19 Jan 2023

Bluebottle cyber crime group active in Africa

''In the last few months, Bluebottle, a notorious cyber crime group has had entities in the financial sector in its crosshairs. Targets are in French-speaking African countries and have been hit by a combination of spear phishing attacks, as well a malware using job opportunities, as a lure. […] Statistics reveal that there were multiple infections of GU Loader malware downloading various tools such as CobaltStrike and .NET loaders, in the Central African Republic between August to October last year.'' READ MORE

Source: All Africa

Date:28 Jan 2023

Seychelles Police Force to Set Up Cybercrime Unit - Assisted by Interpol

"The setting up of a cybercrime unit in Seychelles was the subject of discussions held from Wednesday to Friday between the Seychelles Police Force and a delegation from Interpol. The head of Detective Services in Seychelles, Superintendent Jeffery Antoine, said that such a unit is necessary to deal with the alarming number of cases where people have been duped and scammed out of large sums of money online. […] The superintendent said that initiative is a result of the Cybercrime Act 2021." READ MORE

Source: The Record

Date:24 Jan 2023

Pakistani authorities investigating if cyberattack caused nationwide blackout

''BANGKOK (The Nation/Asia News Network): Almost 120,000 telephone numbers and 60,000 bank accounts operated by criminals were frozen last year, government spokesperson Rachada Dhnadirek said on Thursday (Jan 19). The criminal channels were suspended as part of efforts by the Digital Economy and Society Ministry, police force and other agencies to tackle cybercrimes. Investigators also shut down eight criminal account-trading groups on social media and 1,830 gambling websites last year. READ MORE

Source: The Star

Date:20 Jan 2023

Scale of Thai cybercrime revealed as almost 60,000 bank accounts frozen

''BANGKOK (The Nation/Asia News Network): Almost 120,000 telephone numbers and 60,000 bank accounts operated by criminals were frozen last year, government spokesperson Rachada Dhnadirek said on Thursday (Jan 19). The criminal channels were suspended as part of efforts by the Digital Economy and Society Ministry, police force and other agencies to tackle cybercrimes. Investigators also shut down eight criminal account-trading groups on social media and 1,830 gambling websites last year. The Anti-Money Laundering Office (Amlo) has launched a crackdown against criminals opening bank accounts, she added. The National Broadcasting and Telecommunication Commission has also asked around 8,000 people who own more than 100 smartphone SIM cards to verify their identities by the end of this month in a bid to tackle call centre scams, Rachada said.'' READ MORE

Source: Bankinfosecurity

Date: 23 Jan 2023

Australia Initiates Global Ransomware Task Force Operations

"A global ransomware task force led by Australia and comprised of 37 like-minded governments commenced operations Monday with the aim of sharing intelligence to stymie future digital extortion attacks. The task force is an outgrowth of the U.S.-led Counter Ransomware Initiative, which last met in November at the White House. The task force aims to foster collaboration in global law enforcement agencies and cybersecurity authorities. In addition to swapping intelligence, it will share best practices policy and legal authority frameworks. The global initiative is hosted by the Australian Department of Home Affairs and its recently formed Cyber and Critical Technology Coordination Center." READ MORE

Source: The Record

Date: 31 Jan 2023

Pro-Russian DDoS attacks raise alarm in Denmark, U.S.

"Distributed denial-of-service (DDoS) attacks by pro-Russian hacking groups are causing alarm in the U.S. and Denmark after several incidents affected websites of hospitals and government offices in both countries. On Tuesday, Denmark announced that it was raising its cyber risk alert level after weeks of attacks on banks and the country's defense ministry. Since Russia began its invasion of Ukraine 11 months ago, hacking groups like Killnet and NoName057 have targeted an array of government institutions, businesses and organizations across Europe and the United States. On Monday, Killnet directed DDoS traffic against the websites of dozens of U.S. hospitals, forcing the the U.S. Department of Health and Human Services to publish an alert warning healthcare institutions about the group's tactics." READ MORE

RELATED ARTICLE:

U.S. Department of Health and Human Services, Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector, 30 January 2023

Source: UK National Cybersecurity Center

Date: 26 Jan 2023

UK cyber experts warn of targeted phishing attacks from actors based in Russia and Iran

''The UK has today (Thursday) warned of the threat from targeted spear-phishing campaigns against organisations and individuals carried out by cyber actors based in Russia and Iran. In an advisory published today, the National Cyber Security Centre (NCSC) – a part of GCHQ – shared details about the techniques and tactics used by the attackers as well as mitigation advice to combat the continuing threat. Spear-phishing involves an attacker sending malicious links, for example via email, to specific targets in order to try to induce them to share sensitive information.'' READ MORE

Source: EuroNews

Date: 26 Jan 2023

Russian hackers launch cyberattack on Germany in Leopard retaliation

"The websites of key German administrations, including companies and airports, have been targetted by cyberattacks, the Federal Cybersecurity Agency (BSI) said on Thursday. The BSI has been informed of "DDoS attacks (by denial of service) currently in progress against targets in Germany", said a spokesperson. "Individual targets in the financial sector" and federal government sites were also attacked, with no major consequences at this stage. Denial of Service (DDoS) attacks involve targetting a computer system by flooding it with messages or connection requests.Russian hacker site Killnet has taken credit for the attack, according to the BSI. Handelsblatt media group reported that the attacks were a retaliation against Berlin approving the deployment of Leopard 2 tanks to Ukraine. Clearly identifying where an attack like this comes from, however, is "particularly difficult for hacker collectives", added the BSI spokesperson." READ MORE

Source: The Record

Date: 28 Jan 2023

Latvia confirms phishing attack on Ministry of Defense, linking it to Russian hacking group

"The Russian cyber-espionage group known as Gamaredon may have been behind a phishing attack on Latvia's Ministry of Defense last week, the ministry told The Record on Friday. Hackers sent malicious emails to several employees of the ministry, pretending to be Ukrainian government officials. […] The attempted cyberattack was unsuccessful, the ministry added. The company obtained it from VirusTotal, a Google-owned service that analyzes suspicious files, where one of the targeted users may have downloaded it to verify its sender, according to Sekoia threat intelligence researcher Felix Aime." READ MORE

Source: Reuters

Date: 25 Jan 2023

Dutch hacker obtained virtually all Austrians' personal data, police say

"A Dutch hacker arrested in November obtained and offered for sale the full name, address and date of birth of virtually everyone in Austria, the Alpine nation's police said on Wednesday. A user believed to be the hacker offered the data for sale in an online forum in May 2020, presenting it as "the full name, gender, complete address and date of birth of presumably every citizen" in Austria, police said in a statement, adding that investigators had confirmed its authenticity. The trove comprised close to nine million sets of data, police said. Austria's population is roughly 9.1 million." READ MORE

Latest reports

- European Commission, Study on cross-border use of evidence in criminal proceedings, 10 January 2023
- Chainalysis, 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking, 12 January 2023
- Axios, Ransomware gangs are starting to ditch encryption, 13 January 2023
- TrendMicro, Earth Bogle, Campaigns Target the Middle East with Geopolitical Lures, 17 January 2023
- Human Security, Traffic signals: The VASTFLUX Takedown, 19 January 2023
- BBC News, Cyber-crime gangs' earnings slide as victims refuse to pay, 19 January 2023
- Chainalysis, Ransomware Revenue Down As More Victims Refuse to Pay, 19 January 2023
- Technology and Democracy, Mythbusting: Cybercrime versus Cybersecurity, 20 January 2023
- BCS, Presenting digital evidence in court, 23 January 2023
- ARMIS, Armis State of Cyberwarfare and Trends Report: 2022-2023, 24 Jan 2023
- Opinion Nigeria, Cyber Crime In Nigeria: Yahoo Yahoo As A Case Study, 26 January 2023
- TechTarget, 34 cybersecurity statistics to lose sleep over in 2023, 26 January 2023
- Microsoft Security Blog, 2023 identity security trends and solutions from Microsoft, 26 January 2023
- ENISA, Engineering Personal Data Sharing, 27 January 2023
- IT Wire, Australia named the country 4th most at-risk of cyber crime in the world, 27 January 2023
- Utility Dive, EVs are more popular than ever. They're also extremely prone to cyberattacks, 27 January 2023
- Business Tech, Shift in ransomware attacks – South Africa and emerging markets more at risk, 30 January 2023
- SecureList, Come to the dark side: hunting IT professionals on the dark web, 30 January 2023
- Trusted Sec, New attacks, old tricks: how OneNote malware is evolving, 31 January 2023

Upcoming events

- 1 February, C-PROC/ALBANIA, *(in-person),* Domestic workshop on sharing electronic evidence on international investigations, iPROCEEDS-2
- 1-15 February, C-PROC, (*on-line*) Further work on the Cyberviolence online portal, Octopus
- 2 February, C-PROC/BELGIUM, *(in-person*), GLACY+ Internal Steering Committee, GLACY+
- 3 February, C-PROC/GLACY+, *(in-person*), GLACY+ 13th Steering Committee, GLACY+
- 6-8 February, C-PROC/RWANDA, (*in-person*), Advisory mission on legislation, GLACY+
- 7-10 February, C-PROC/ARMENIA, *(in-person),* First Responder Training for Investigators on Cybercrime and Electronic Evidence*,* CyberEast
- 14-16 February, C-PROC/PORTUGAL, *(in-person*), Regional training on Joint Investigative Teams (JITs) and improved cooperation with foreign service providers under the Second Additional Protocol to the Budapest Convention, iPROCEEDS-2, CyberEast, GLACY+, CyberSouth, Octopus
- 15-16 February, C-PROC/SINGAPORE, *(on-line),* Participation in the INTERPOL Global Cybercrime Conference, GLACY+
- February, C-PROC, Finalization of the study on good practices in implementation or reflection of the First Additional Protocol to the Convention on Cybercrime, Octopus