Cybercrime Digest

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

16 – 31 October 2021

Source: Council of Europe

Date: 28 Oct 2021

Special event on the 20th anniversary of the Budapest Convention and the forthcoming Protocol: Update

"The special event on the occasion of the 20th anniversary of the Budapest Convention on Cybercrime and the forthcoming Second Additional Protocol will be held online on 16 November, from 13h00 to 18h00 (France). Speakers from around the world […] will share their views on the impact of the Convention and expectations related to the future Protocol. Registration for the Conference is open until 7 November." READ MORE

Source: Europol

Date: 26 Oct 2021

150 arrested in dark web drug bust as police seize €26 million

"Police forces across the world have arrested 150 alleged suspects involved in buying or selling illicit goods on the dark web as part of a coordinated international operation involving nine countries. More than €26.7 million (USD 31 million) in cash and virtual currencies have been seized in this operation, […]. This operation, known as Dark HunTOR, was composed of a series of separate but complementary actions in Australia, Bulgaria, France, Germany, Italy, the Netherlands, Switzerland, the United Kingdom and the United States, with coordination efforts led by Europol and Eurojust." READ MORE

RELATED ARTICLE:

US Department of Justice, International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in 150 Arrests Worldwide and the Seizure of Weapons, Drugs, and over $31 Million, 26 October 2021

Source: Wall Street Journal

Date: 25 Oct 2021

Updated Cybercrime Pact Aims to Speed Cross-Border Investigations

"Proposed changes to the Budapest Convention are an attempt to inject some alacrity into sluggish cross-jurisdictional inquiries that give hackers time to disappear along with evidence. […] The main changes to the Budapest Convention, in effect since 2004, focus on updating investigative tools that are too slow to be effective in cybercrime cases, where hackers move quickly and data can disappear. Under the revised agreement, new legal channels would make it easier for prosecutors and police to obtain digital evidence quickly by directly contacting technology companies outside their jurisdiction, according to cybercrime experts." READ MORE

Source: Europol

Date: 29 Oct 2021

12 targeted for involvement in ransomware attacks against critical infrastructure

"A total of 12 individuals wreaking havoc across the world with ransomware attacks against critical infrastructure have been targeted as the result of a law enforcement and judicial operation involving eight countries. These attacks are believed to have affected over 1 800 victims in 71 countries." READ MORE

Source: Interpol

Date: 28 Oct 2021

Increasing cybercrime threats focus of INTERPOL's regional policing dialogue

"Gathering at the INTERPOL Dialogue, leaders of regional policing bodies discussed the need for a more effective and coordinated response to tackle cybercrime and other transnational threats. The growing trend of 'cybercrime as a service', with more sophisticated, more complete and more accessible packages of services and tools lowering the barriers to entry for would-be cybercriminals, was identified as key development Addressing the two-day (27 and 28 October) meeting hosted at the Arab Interior." READ MORE

Source: krebsonsecurity.com

Date: 25 Oct 2021

Conti Ransom Gang Starts Selling Access to Victims

"The Conti ransomware affiliate program appears to have altered its business plan recently. Organizations infected with Conti's malware who refuse to negotiate a ransom payment are added to Conti's victim shaming blog, where confidential files stolen from victims may be published or sold. But sometime over the past 48 hours, the cybercriminal syndicate updated its victim shaming blog to indicate that it is now selling access to many of the organizations it has hacked." READ MORE

RELATED ARTICLE:

REUTERS, Governments turn tables on ransomware gang REvil by pushing it offline, 22 October 2021

Source: BleepingComputer

Date: 28 Oct 2021

German investigators identify REvil ransomware gang core member

"German investigators have reportedly identified a Russian man whom they believe to be one of REvil ransomware gang's core members, one of the most notorious and successful ransomware groups in recent years. […] While the suspect's real identity has not been revealed, German media is calling him by the fictitious name 'Nikolay K.', and report that investigators linked him to Bitcoin ransom payments associated with the GandCrab ransomware group. […] Nikolay K. didn't hold back when it came to boasting on social media and showcasing his holidays on the Mediterranean, posting images from lavish yacht parties." READ MORE

RELATED ARTICLE:

Tageschau, Verdächtiger in Russland identifiziert, 28 October 2021

Source: portal.ieu-monitoring.com

Date: 29 Oct 2021

Cybersecurity: MEPs strengthen EU-wide requirements against threats

"[…] According to the legislative text adopted on Thursday by the Industry Committee, EU countries would have to meet stricter supervisory and enforcement measures and harmonize their sanctions regimes. Compared to the existing legislation, the new directive would oblige more entities and sectors to take measures. […] In addition, the new rules would also protect so-called "important sectors" such as postal services, waste management, chemicals, food, manufacturing of medical devices, electronics, machinery, motor vehicles and digital providers. READ MORE

Source: Council of Europe

Date: 19 Oct 2021

Council of Europe and EUROJUST: Workshop on Joint Investigation Teams/Joint Investigations

"On 19th of October 2021, EuroJust and the Council of Europe, through the Cybercrime Programme Office (C-PROC), organized a Joint Workshop on International Cooperation in Cybercrime: Joint Investigation Teams/Joint Investigations, bringing together approximately 150 representatives of law enforcement authorities, prosecution service and central authorities responsible for judicial cooperation." READ MORE

Source: Eurojust

Date: 27 Oct 2021

Support for the arrest of online scammers in Georgia and Israel

"With Eurojust's support, authorities in Germany, Georgia and Israel have dismantled a criminal network operating various online trading platforms, defrauding victims of at least tens of millions of euros. During a series of actions in Georgia and Israel last week, 11 suspects were arrested, and real estate, luxury vehicles, communication equipment and cash were seized, for a yet unknown amount. Investigations into the fraud scheme started in 2015, after complaints from citizens, including German victims, who had lost all their investments via at least 18 different online trading platforms." READ MORE

Source: protecciondatos.mx

Date: 25 Oct 2021

Webinars en países de LATAM sobre el Segundo Protocolo Adicional del Convenio de Budapest

"El Proyecto Octopus del Consejo de Europa en cooperación con el Proyecto GLACY + está organizando una serie de seminarios web y mesas redondas con múltiples partes interesadas en la región de América Latina y el Caribe (ALC) durante octubre y noviembre de 2021 y enero de 2022 con el objetivo de difundir y generar los beneficios del Segundo Protocolo Adicional sobre cooperación reforzada y divulgación de pruebas electrónicas que fue aprobado por el Comité de Expertos del Convenio de Budapest (T-CY) el 31 de mayo de 2021." READ MORE

Source: Council of Europe

Date: 20 Oct 2021

Trinité et Tobago sur la voie de l'adhésion à la Convention de Budapest

"Trinité et Tobago a été invité par le Conseil de l'Europe à adhérer à la Convention de Budapest sur la cybercriminalité. Plus tôt cette année, Trinté et Tobago a participé à des activités dans le cadre du projet Octopus à l'appui des réformes de la législation nationale sur la cybercriminalité. " READ MORE

Source: AGESIC

Date: 21 Oct 2021

Uruguay: Taller en línea sobre el Convenio Budapest

"El 20 de octubre se realizó un taller virtual de alto nivel, del que participaron más de 70 representantes de organismos nacionales, con el objetivo de identificar soluciones para fortalecer la capacidad del país en materia de ciberdelitos. Autoridades nacionales, internacionales, representantes del poder legislativo, jueces y fiscales formaron parte de la actividad organizada por Agesic junto con la Oficina de Lucha contra la ciberdelincuencia del Consejo de Europa, en el marco del proyecto Global Action on Cybercrime Extended (GLACY+), un proyecto conjunto de la Unión Europea y del Consejo de Europa." READ MORE

Source: lexpress.mu

Date: 22 Oct 2021

Maurice : Conseil des ministres: un Cybersecurity and Cybercrime Bill présenté au Parlement

"Un projet de loi sur la cybersécurité et le cybercrime sera présenté à l'Assemblée nationale (qui reprend ses travaux mardi 26 octobre). Son principal objectif est de remplacer la *Computer Misuse and Cybercrime Act*. Il fera notamment provision pour de nouveaux délits criminels relatifs au cybercrime et à la cybersécurité, avec des techniques d'enquête améliorées et une coopération internationale accrue. Seront aussi mis en place une *Critical Information Infrastructure Protection policy*, un *National Cybersecurity Committee*." READ MORE

Source: Council of Europe

Date: 18-22 Oct 2021

GLACY+: Streamlining procedures for Mutual Legal Assistance and enhancing international cooperation in Ghana

"The GLACY+ project, a joint action of the European Union and the Council of Europe supported the Ghanaian authorities, particularly the Cyber Security Authority, in organising two back-to-back activities focused on enhancing international cooperation on cybercrime in Accra, Ghana, in a hybrid format. […] The mission examined areas which may require further capacity building support through the GLACY+ project and highlighted ways to streamline procedures for MLA related to cybercrime and electronic evidence." READ MORE

Source: Council of Europe

Date: 26 Oct 2021

CyberSouth: National workshop on developing a cybercrime reporting mechanism in Morocco

"On 26 October 2021, the CyberSouth project organised for Moroccan stakeholders the second national workshop in the series intended to support the development of a dedicated cybercrime reporting mechanism in the priority countries. The workshop provided an overview of the role of cybercrime reporting mechanism, its structure and methods of collection, as well as the impact of reports on information sharing and investigative process." READ MORE

Source: BBC News

Date: 20 Oct 2021

Nigerian romance scam suspects targeted 100 women - FBI

"Eight Nigerian men accused of an internet dating scam have appeared in a South African court after a massive international operation involving the FBI and Interpol. […] They are accused of defrauding more than 100 victims of almost $7m (£5m) in total over the past decade." READ MORE

Source: BleepingComputer

Date: 26 Oct 2021

Iranian gas stations out of service after distribution network hacked

"Gas stations from the National Iranian Oil Products Distribution Company (NIOPDC) have stopped working today due to a cyberattack that affected the entire distribution network. The incident has generated a string of hacks on electronic road billboards to show messages demanding an explanation or asking for fuel. The NIOPDC network has more than 3,500 stations across the country and has been supplying oil products for more than 80 years." READ MORE

Source: telenganatoday.com

Date: 21 Oct 2021

India: Telangana to have law on cybercrime soon

"Telangana, known for its pioneering initiatives in various fields, is now heading towards becoming the first State in the country to have its own legislation on cybercrime. The draft legislation is being prepared with the help of Nalsar, Hyderabad-based premier law institute, IT and Industries Minister KT Rama Rao said on Thursday. "Telangana will be the first State in the country to draft out its own legislation on cybercrime. […]," he said […]" READ MORE

Source: ZDNet

Date: 21 Oct 2021

450 million cyberattacks attempted on Japan Olympics infrastructure: NTT

"The NTT Corporation, which provided wide-ranging telecommunications services and network security for the Olympic & Paralympic Games in Tokyo this summer, said there were more than 450 million attempted cyberattacks during the event in July. NTT officials said none of the attacks were successful and added that the games went on without a hitch. But the number of attacks was 2.5x the number seen during the 2012 London Summer Olympics." READ MORE

Source: RZN

Date: 21 Oct 2021

PNG government system hit by ransomware attack

"Papua New Guinea's government pay system has been hit by a ransomware cyber-attack. The finance minister and acting treasurer, John Pundari, confirmed that the attack on the Department of Finance's Integrated Financial Management System occurred a week ago. The system, which manages access to hundreds of millions of dollars in foreign aid money, was disabled by attackers who demanded Bitcoin in ransom payment from PNG. Pundari said the government didn't pay a ransom to any hacker or third party, adding that the system had now been "fully restored"." READ MORE

Source: CoinDesk

Date: 21 Oct 2021

Australian Senate Committee Calls for New Rules for Crypto

"An Australian Senate committee has recommended a set of new rules to establish a clear framework for the country's digital assets sector. The committee on "Australia as a Technology and Financial Centre," which submitted its initial report on the topic last November and a second in April this year, presented its third and final report Tuesday. The document outlines problems identified by leading industry participants and includes 12 recommendations to address the lack of crypto and blockchain regulations in the country. […] The committee recommended implementing a new licensing regime for crypto exchanges and establishing a custody or depository regulatory framework for digital assets." READ MORE

Source: BleepingComputer

Date: 23 Oct 2021

Hacker sells the data for millions of Moscow drivers for $800

"Hackers are selling a stolen database containing 50 million records of Moscow driver data on an underground forum for only $800. According to Russian media outlets that purchased the database, the data appears to be valid and contains records collected between 2006 and 2019. […] The database contains the following details on Moscow car owners: Full names, Dates of birth, Phone numbers, VIN codes, License plate numbers, Car brand and model, Car year of registration." READ MORE

Source: Threat Post

Date: 28 Oct 2021

EU's Green Pass Vaccination ID Private Key Leaked

"French & Polish authorities found no sign of cryptographic compromise in the leak of the private key used to sign the vaccine passports and to create fake passes for Mickey Mouse and Adolf Hitler, et al. […]On Wednesday, the Italian news agency ANSA reported that several underground vendors were selling passes signed with the stolen key on the Dark Web, and that the EU had called "several high-level meetings" to investigate whether the theft was an isolated incident." READ MORE

Source: portswigger.net

Date: 25 Oct 2021

EU ban on anonymous domain registration welcomed by threat intel firm

"Forthcoming European Union regulations that would curtail anonymous domain registration has been welcomed by a security firm despite concerns from some including Germany's top-level domain registry, DENIC. Wide-ranging proposals to achieve a "high common level of cybersecurity across the Union" and update the 2016 network and information systems (NIS Directive), would restrict the anonymous registration of domains, among other measures. Anonymous domain registration is often associated with illegal activities including the distribution of malware and the hosting of phishing sites as well as the authorized distribution of copyright protected works." READ MORE

Source: Ofcom

Date: 20 Oct 2021

UK: 45 million people targeted by scam calls and texts this summer

"Almost 45 million people have been on the receiving end of potential scam texts or calls in the last three months, new Ofcom research reveals. More than eight in 10 (82%) said they had received a suspicious message, in the form of either a text, recorded message or live phone call to a landline or mobile. This represents an estimated 44.6 million adults in the UK. Scams are more commonly attempted via text messages with seven in 10 people (71%) saying they have received a suspicious text, and three quarters (75%) of those aged 16-34 were targeted." READ MORE

Source: Observador

Date: 20 Oct 2021

Portugal: Pandemia deslocalizou criminalidade da rua para espaço digital, aponta ministra

"Ministra referiu que a pandemia criou condições para os grupos criminosos organizados centrarem a sua ação em atividades ilícitas cuja rentabilidade aumentou, nomeadamente na área da saúde. A ministra da Justiça alertou esta quarta-feira que a pandemia de Covid-19 gerou condições para a deslocalização da criminalidade da rua para o espaço digital, designadamente a criminalidade informática, as fraudes cometidas em ambiente informático e a divulgação de pornografia infantil. […] Esta nova realidade, disse, "reclama uma reação pronta, eficaz e efetiva, que só se pode concretizar com recurso a meios idóneos: a dimensão pericial a permanente atualização tecnológica"." READ MORE

Latest reports

- Microsoft, Digital Defense Report, October 2021
- Money.co, Quarterly Fraud and Cyber Crime Report, 15 October 2021
- Cybersecuritymag-Africa, Google analyse 80 millions d'échantillons de ransomware : voici ses conclusions, 18 October 2021
- Kasperski, Russian-speaking cybercrime evolution: what has changed in recent years?, 20 October 2021
- Embroker.com, 2021 Must-Know Cyber Attack Statistics and Trends, 20 October 2021
- Securelist.com, Russian-speaking cybercrime evolution: What changed from 2016 to 2021, 20 October 2021
- APNIC Asia-Pacific, How to: Threat hunting and threat intelligence, 21 October 2021
- Interpol, INTERPOL report identifies top cyberthreats in Africa, 25 October 2021
- FBI, FBI warns of Ranzy Locker ransomware threat, as over 30 companies hit, 25 October 2021
- L'expert comptable.com, Les enjeux de la cyber sécurité en entreprise, 25 October 2021
- Portswigger, Africa sees increase in ransomware, botnet attacks – but online scams still pose biggest threat, 26 October 2021
- Cyberark, Cracking WiFi at Scale with One Simple Trick, 26 October 2021
- Coalition for a Secure and Transparent Internet, ICANN 72 Summary of WHOIS and Proxy Requests Under GDPR DNS Abuse Framework Requests, 26 October 2021
- La finance pour tous, Comment se protéger (un peu) contre la cybercriminalité, 27 October 2021
- Enisa Europa, Enisa Threat Landscape 2021, 27 October 2021
- Interpol, Ground-breaking insights into the risk of online child sexual exploitation and abuse in Kenya, 28 October 2021

Upcoming events

- 2 November, C-PROC/ALGERIA, (*online*), National Workshop on the development of the dedicated cybercrime reporting mechanism, CyberSouth
- 3 November, C-PROC, (*online*), Series of monthly thematic webinars for the International Network of the National Judicial Trainers, GLACY+
- 5 November, C-PROC, (*online*), 1st multistakeholder webinar in the series of webinars on the 2nd Additional Protocol to the Budapest Convention in the Latin America region, OCTOPUS, GLACY+
- 8 November, Advisory mission on development of Standard Operating Procedures in South Africa, EU-SA Dialogue Facility Project in cooperation with OCTOPUS
- 8 November (TBC), C-PROC, (*desk assessment),* Continuation of the needs assessment meetings in pilot countries/institutions: the case for an online training platform, OCTOPUS
- 8-10 November, C-PROC/UKRAINE, (*online*), Training on interagency cooperation and financial investigations/intelligence, CyberEast
- 8-12 November, C-PROC/GEORGIA and ARMENIA, Supporting TOPCOP project training on Darkweb for Georgian and Armenian investigators, (Budapest), CyberEast

- 8 November, C-PROC/TURKEY, *(online*), Workshop on the role, set-up and competencies of the 24/7 points of contact in Turkey, iPROCEEDS-2
- 9 November, C-PROC/LATAM and CARIBBEAN, (*online*), Implementers and Donors Forum - GFCE Americas Regional Hub, GLACY+9 November, C-PROC, (*online*),Third Meeting of the CyberSouth Judicial Network, CyberSouth
- 9 November (TBC), C-PROC, (*online*), Final Story Board meeting on development of the HELP Course on Cybercrime and electronic evidence, OCTOPUS
- 9 November, C-PROC, (*online*), 1st Regional Roundtable on COVID-19 related Cybercrime in Asia, OCTOPUS
- 9-10 November, C-PROC/GHANA, (*online*), Meeting of Cybercrime Unit Heads for ECOWAS region and Mauritania, GLACY+
- 11 November, C-PROC, (*online*), Participation in the Europol-INTERPOL Annual Cybercrime Conference, CyberSouth
- 11-13 November, C-PROC, (*online*), GLACY+ Project showcased in the Paris Peace Forum, GLACY+
- 15 November, C-PROC, (*online*), 25th T-CY Plenary meeting, T-CY and OCTOPUS

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 November 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