Cybercrime Digest

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

01 – 15 September 2021

Source: Bloomberg

Date: 09 Sep 2021

UN Computer Networks Breached by Hackers Earlier This Year

““[…]“We can confirm that unknown attackers were able to breach parts of the United Nations infrastructure in April of 2021,” Stéphane Dujarric, spokesman for the UN Secretary-General said […]. “The United Nations is frequently targeted by cyberattacks, including sustained campaigns. We can also confirm that further attacks have been detected and are being responded to, that are linked to the earlier breach.” The credentials belonged to an account on the UN’s proprietary project management software, called Umoja. From there, the hackers were able to gain deeper access to the UN’s network, according to cybersecurity firm Resecurity, which discovered the breach.’’ READ MORE

Source: Eurojust

Date: 09 Sep 2021

Coordinated action against international investment fraud network

“[…] Coordinated searches and witness hearings in Palma de Mallorca (Spain), the Netherlands, Sweden and Denmark took place to halt the activities of a criminal group committing large-scale investment fraud, causing damages amounting to over EUR 55 million to a large number of victims across Europe. […] Using a series of false websites, the criminal network deceived a large number of victims by selling false financial investment products, shares and bonds while never actually investing the money it received.” READ MORE

Source: Council of Europe

Date: 09 September 2021

2nd edition of Member state responses to prevent and combat OCSEA is out with new data and recommendations

“The Council of Europe Project “End Online Child Sexual Exploitation and Abuse @ Europe” (EndOCSEA@Europe), has published the second edition of the Baseline Mapping of member state responses to prevent and combat online child sexual exploitation and abuse. The Report builds upon the structure and rationale of the first edition, developed by Dr Victoria Baines, Council of Europe expert, and published in 2019. The second edition includes new information and data, in particular in the context of the COVID-19 pandemic.” READ MORE

Source: BBC

Date: 03 Sep 2021

Apple delays plan to scan iPhones for child abuse

“Apple said that it had listened to the negative feedback and was reconsidering. There were concerns the system could be abused by authoritarian states. The so-called NeuralHash technology would have scanned images just before they are uploaded to iCloud Photos. Then it would have matched them against known child sexual abuse material on a database maintained by the National Center for Missing and Exploited Children. If a match was found then it would have been manually reviewed by a human and, if required, steps taken to disable a user's account and report it to law enforcement. It was due to launch later in the year. READ MORE

Source: Ireland's National Public Service Media

Date: 02 Sep 2021

Record €225m fine for WhatsApp Ireland over data protection breaches

"The Data Protection Commission (DPC) has fined WhatsApp Ireland €225m for infringements of data protection rules. It is the largest fine ever imposed by the DPC and the second largest penalty ever levied on an organisation under EU data laws.
The regulator has also ordered the messaging service to bring its processing into compliance by taking a range of specified remedial actions. WhatsApp has said it disagrees with the decision, has claimed the penalties are entirely disproportionate and has stated it will appeal the ruling." READ MORE

Source: US Department of Justice

Date: 08 Sep 2021

International money launderer sentenced to federal prison in cyber-crime conspiracies responsible for intended loss of nearly $60 million

"A Canadian man who conspired to launder tens of millions of dollars stolen in various wire and bank fraud schemes – including a massive online banking theft by North Korean cyber criminals – has been sentenced to nearly 12 years in federal prison. […] "This defendant served as an integral conduit in a network of cybercriminals who siphoned tens of millions of dollars from multiple entities and institutions across the globe," said Acting U.S. Attorney Estes. "He laundered money for a rogue nation and some of the world's worst cybercriminals, and he managed a team of co-conspirators who helped to line the pockets and digital wallets of thieves. […]"." READ MORE

Source: Kaspersky

Date: 31 Aug 2021

Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021

"El Home Office (acceso remoto) y la piratería son los principales vectores de ataque, tanto para consumidores como para empresas. Las principales amenazas que asechan a la región generan un promedio de 35 ataques por segundo. […]La tendencia de crecimiento en ciberataques también se refleja en todos los países, con la excepción de Costa Rica, que registró un leve aumento del 2%. La lista de países la lidera Ecuador (+75%), seguido por Perú (+71%), Panamá (+60%), Guatemala (+43%) y Venezuela (+29%). En total, solo el Top20 de malware en la región genera un promedio de 35 ataques por segundo.'' READ MORE

Source: New Scientist

Date: 10 Sep 2021

Why has El Salvador officially adopted bitcoin as its currency?

"President Nayib Bukele hopes bitcoin will alleviate El Salvador's prickliest economic problems: citizens sending money home from abroad account for up to a fifth of the country's GDP, but they have to pay high transaction costs, and 70 per cent of people have no bank account. Bitcoin enables quick, cheap payments across borders, and doesn't require banks. Every Salvadoran has been gifted $30 in bitcoin (the US dollar is the nation's other official currency) and can now shop or pay their taxes with it. Companies must accept it by law but are permitted to instantly swap all bitcoin to dollars once received." READ MORE

RELATED ARTICLE:

BBC, Bitcoin: El Salvador divided over legal tender law, 03 September 2021

Source: ZDNet

Date: 13 Sep 2021

Brazil debates creation of national strategy to tackle cybercrime

"The president at the Brazilian Federation of Banks (FEBRABAN), Isaac Sidney, and the Minister of Justice and Public Security, Anderson Torres, have started negotiations for the creation of the National Cybercrime Strategy. […] The vision outlined by the banking association also includes the joint development of platforms for sharing fraud data by digital means and supporting the training of security forces in cybersecurity and digital fraud issues, and using the association's cybersecurity laboratory. The plan would also include public awareness campaigns on cyber risks and fraud.'' READ MORE

Source: RFI

Date: 08 Sep 2021

Le gouvernement ivoirien durcit les peines en matière de cybercriminalité

"Ce genre de cas est de plus en plus fréquent au tribunal d'Abidjan, et les peines devraient encore s'alourdir désormais. Les peines maximales dans certains cas vont être multipliées par deux par rapport à celles prévues dans la loi de 2013 sur la cybercriminalité a expliqué ce mercredi le porte-parole du gouvernement Amadou Coulibaly. Sont particulièrement visés les comportements sur les réseaux sociaux, comme les outrages et invectives punis jusque-là de cinq ans de prison, tout comme les publications de nature à troubler à l'ordre public." READ MORE

Source: Africa News

Date: 14 Sep 2021

Kaspersky records over 2 million phishing attacks in South Africa, Kenya and Nigeria in H1 2021 and spam email still a threat

"There was a reduction in the number of phishing attacks recorded and blocked by Kaspersky (www.Africa.Kaspersky.com)in South Africa (17% decline), Kenya (48% decline), and Nigeria (13% decline) for the first half of this year when compared to the same period in 2020. While the decline does suggest and support research trends – that cybercriminals have become more targeted, focusing their efforts on advanced persistent threat (APT) campaigns in Africa – the phishing threat is still very prevalent, says Kaspersky. […] Reaching over two million attacks combined highlights that phishing is still a significant threat in Africa and illustrates the importance of ensuring cybersecurity solutions are installed on all connected devices." READ MORE

Source: OpenGov Asia

Date: 08 Sep 2021

Philippine Bill Introduced to Combat Cybercrimes in the Finance Sectors

"[…] a Philippine senator has introduced new legislation to combat new cybercrimes such as skimming and phishing, which have reached an all-time high since most transactions have shifted online during the pandemic. The "Bank Account, E-wallet, and Other Financial Accounts Regulation Act," also known as Senate Bill No. 2380, aims to promote and maintain a stable and efficient financial system while also recognising the need to protect the public from cybercriminals and syndicates that target bank accounts and e-wallets. […] The measure aims to ensure that the hard-earned money of the public is kept safe and that public trust and confidence in the nation's financial system are maintained as it continues to innovate and traverse through cyberspace, said the senator." READ MORE

Source: The Register

Date: 01 Sep 2021

Indonesian authorities probe million-record leak from national COVID app

"Indonesia's Ministry of Communications and Informatics is investigating a leak of over a million records from the nation's COVID-19 quarantine management app. News of the leak was revealed on August 30th by security review site vpnMentor, which wrote that its research team discovered exposed databases generated by eHAC, an app that is mandatory for use by travelers moving into and out of Indonesia, or within its borders." READ MORE

Source: Reuters

Date: 15 Sep 2021

Cybercrime spreads in Australia as COVID-19 pushes more people online

"Australia reported on Wednesday a 13% jump in cyber-crime in the past year, with about one incident in four targeting critical infrastructure and services as working from home during the pandemic made more people vulnerable to online attacks.[…] The Australian Cyber Security Centre (ACSC) received one cybercrime report every eight minutes over the 12 months to June 30, 2021, it said in its annual report. Hackers have switched their focus to people working remotely online, and used fear created by COVID-19 to actively target vulnerable people and health services to conduct espionage, and steal money and sensitive data, Assistant Minister of Defence Andrew Hastie said in a statement." READ MORE

RELATED ARTICLE:

The Guardian, 'Significant threat': cyber-attacks increasingly targeting Australia's critical infrastructure, 14 September 2021

Source: Le Figaro

Date: 07 Sep 2021

Émoi après que la messagerie sécurisée ProtonMail a collaboré à une enquête judiciaire

" «Proton se défend en disant que la France utilise des dispositions antiterroristes. C'est complètement faux», a commenté sur Twitter l'officier de gendarmerie Matthieu Audibert. «La Suisse a signé la Convention de Budapest qui prévoit la collecte des preuves électroniques pour toute infraction pénale. La Suisse a également des accords de coopération avec Europol. Donc en pratique, nous avons une demande de coopération qui part vers Europol, qui arrive en Suisse, la justice suisse dit OK et Proton répond à la demande via la justice suisse et Europol», explique-t-il. «Cela n'a rien à voir avec les lois françaises antiterroristes. C'est du droit commun régissant l'obtention des preuves numériques.»" READ MORE

Source: Reuters

Date: 06 Sep 2021

British watchdog demands more power over crypto promotions

"With some cryptoassets using social media influencers and other celebrities to promote so-called tokens, Britain's finance ministry has already consulted on the need to regulate them. The rapid growth of cryptoassets has created a new and complex market for regulators around the world to police, with some acting to curb the activities of players in the sector. […]"We'll need two streams to tackle the problem of online financial scams: appropriate regulation, including self-regulation by online platforms and robust enforcement by the authorities; and greater consumer awareness about online scams."" READ MORE

Source: ZDNEt

Date: 03 Sep 2021

Fed up with constant cyberattacks, one country is about to make some big changes

“Italy has faced a barrage of cyberattacks in recent weeks. On August 1, the main data center of the Lazio region was hit by a ransomware attack, which made many of its online services, including the COVID-19 vaccination-booking platform, inaccessible. All data was encrypted, and attackers requested a bitcoin ransom to allow authorities to recover them. Luckily, technicians were able to restore the stolen data from a backup copy. […] "The problem is not the tool, but the way it is used," Corrado Giustozzi, a well-known cybersecurity expert in Italy, tells ZDNet. "A great car is useless, if badly driven. We need to focus on improving the processes and the culture."” READ MORE

Source: IT Pro

Date: 08 Sep 2021

Irish police seize Conti domains used in HSE ransomware attack

“Ireland’s Garda National Cyber Crime Bureau has announced that it had “seized several domains” used in the ransomware attack on the Irish Health Service Executive (HSE) earlier this year. […] The Bureau has also notified potential victims of the ransomware gang and is working with Europol and Interpol to ensure that other states are aware of the systems targeted by Conti.” READ MORE

Latest reports

- Helpnetsecurity, Increase in credential phishing and brute force attacks causing financial and reputational damage, 31 August 2021
- Intel471, Outsourcing manipulation: How BEC scammers use the cybercrime underground, 1 September 2021
- Buyouts, There's no silver bullet' - Investors take on the multi-headed beast, 1 September 2021
- Team Cymru, Team Cymru's Threat Hunting Maturity Model Explained, 2 September 2021
- Krebs on Security: Gift Card Gang Extracts Cash From 100k Inboxes Daily, 2 September 2021
- Trip Wire, Data Breaches: A Chance for Opportunistic Scammers & What You Should Watch for, 5 September 2021
- European Commission, Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy, 6 September 2021
- Clyde&Co, Cybercrime – are your employees a threat to operational security?, 6 September 2021
- Schneier on Security, Tracking People by their MAC Addresses, 6 September 2021
- International Journal of Electronic Security and Digital Forensics, Detecting forged video evidence, 7 September 2021
- Cyber Defense Magazine, Considering Collateral Intrusion in Digital Forensics, 7 September 2021
- Comparitech, Dark web prices for stolen PayPal accounts up, credit cards down: report, 8 September 2021
- Kaspersky, Threat landscape for industrial automation systems. Statistics for H1 2021, 9 September 2021
- Fotoware, 7 Common Challenges Police Forces Face When Handling Digital Evidence, 9 September 2021
- Aspen Institute - Diversity, Equity, and Inclusion in Cybersecurity, 9 September 2021
- ENISA, Methodology for a Sectoral Cybersecurity Assessment, 13 September 2021
- Science Direct: Digital evidence: Unaddressed threats to fairness and the presumption of innocence, September 2021
- BlackFog, The State of Ransomware in 2021, September 2021

Upcoming events

- 16 September, C-PROC/ALGERIA, (online), Third Working Group Meeting on the mainstreaming of judicial training material on cybercrime and electronic evidence, CyberSouth
- 17 September, C-PROC/KOSOVO*, (on-line), Needs assessment and improvement/development of functions of the online public reporting system on online fraud and other cybercrime offence in Kosovo*, iPROCEEDS-2
- 17 September, C-PROC/ BOSNIA AND HERZEGOVINA, (on-line), Domestic workshop on MLA practices on country level, alignment of procedures with the Budapest Convention and its Second Additional Protocol, iPROCEEDS-2
- 20 September, C-PROC/ NORTH MACEDONIA, (on-line), Domestic workshop on MLA practices on country level, alignment of procedures with the Budapest Convention and its Second Additional Protocol, iPROCEEDS-2
- 20 September, C-PROC/BURKINA FASO, (online), Advisory mission on legislation with UNOTC, UNODC & OCWAR-C Project, GLACY+
- 20-23 September, C-PROC/UKRAINE, (online), Introductory judicial training for prosecutors, CyberEast
- 21 September, C-PROC/MONTENEGRO, (on-line), Domestic workshop on MLA practices on country level, alignment of procedures with the Budapest Convention and its Second Additional Protocol, iPROCEEDS-2
- 21 September, C-PROC/UNODC, (online), Regional workshop on legislation and capacities of criminal justice authorities to fight online child sexual exploitation in Asia, OCTOPUS
- 21-22 September, C-PROC/INTERPOL, (online), 5th INTERPOL Working Group on Dark Web and Virtual Assets, GLACY+
- 22 September, C-PROC/TURKEY, (on-line), Domestic workshops on cybercrime and cybersecurity trends as well as for criminal justice statistics in each beneficiary, iPROCEEDS-2
- 22 September, C-PROC/TURKEY (desk assignment), Reports on cybercrime and cybersecurity trends as well as for criminal justice statistics in each beneficiary, iPROCEEDS-2
- 24 September, C-PROC/TURKEY, (on-line), Domestic workshop on MLA practices on country level, alignment of procedures with the Budapest Convention and its Second Additional Protocol, iPROCEEDS-2
- 27-30 September, C-PROC/GEORGIA, (online), Introductory judicial training for prosecutors, CyberEast
- 28 September, C-PROC/CARICOM, (online), Series of regional webinars to Promote Universality and Implementation of the Budapest Convention on Cybercrime (2/4), GLACY+, OCTOPUS
- 28 September, C-PROC, Working Group for the development of an online training platform on cybercrime and electronic evidence, OCTOPUS
- 29-30 September, C-PROC/COSTA RICA, (online), Advisory workshop on the streamlining of procedures for mutual legal assistance enhanced by the Second Additional Protocol related to cybercrime and electronic evidence, GLACY+
- 30 September, C-PROC/NORTH MACEDONIA, (on-line and desk research), Workshop on drafting policies and strategies in cybercrime area in line with international standards, iPROCEEDS-2

- By 30 September, C-PROC, (desk research), Comparative analysis of the legislation of Nauru against the provisions of the Budapest and Lanzarote Conventions, GLACY+, OCTOPUS
- By 30 September, C-PROC, Translation of the Specialized Course on International Cooperation into Portuguese language, OCTOPUS
- September–October, C-PROC, (desk research), Preparation of country profiles on OCSEA for Brunei, Cambodia, Indonesia, Laos, Malaysia, Singapore, Thailand, Vietnam, 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 September 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