Cybercrime Digest

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

16 – 28 February 2022

Source: Council of Europe

Date: 25 Feb 2022

Council of Europe suspends Russia's rights of representation

"In line with the Statute of the Council of Europe, the Committee of Ministers has today decided to suspend the Russian Federation from its rights of representation in the Committee of Ministers and in the Parliamentary Assembly with immediate effect as a result of the Russian Federation's armed attack on Ukraine. The decision adopted today means that the Russian Federation remains a member of the Council of Europe and party to the relevant Council of Europe conventions, including the European Convention on Human Rights. [...] The decision was taken following an exchange of views with the Parliamentary Assembly in the Joint Committee." READ MORE

RELATED ARTICLE:

Council of Europe, Situation in Ukraine: Decisions by Council of Europe's Committee of Ministers, 24 February 2022

Council of Europe, Statement from Council of Europe Secretary General Marija Pejčinović Burić on the military attack by the Russian Federation on Ukraine, 24 February 2022

Source: BBC

Date: 28 Feb 2022

Ukraine invasion: How the war is being waged online

"Russia's invasion of Ukraine, it has been said, would be the first to introduce a new front line - the internet. And cyber-attacks have been raging on both sides, with warnings things could escalate. But a digital war is being waged in many other ways too - from questions about whether technology companies should block content to Russia, to online censorship, the spread of disinformation, and Ukraine's internet facing disruption as missiles fall. [...] Pretty much as soon as Russia invaded, Ukraine's politicians began asking the big technology companies so many rely on for information and entertainment to play an active role in the war. [...] Russia's government has imposed partial blockades on Facebook and Twitter, after clashes with the companies." READ MORE

RELATED ARTICLE:

Vice News, Russia's Invasion of Ukraine Is Already Taking Down the Internet, 24 February 2022

Fortune, Russia limits access to Facebook as the social networking giant attempts to fact-check pro-Kremlin propaganda, 26 February 2022

Euractiv, Ukraine: la Commission cherche le «meilleur moyen juridique» pour bannir RT et Sputnik de l'UE, 27 February 2022

Source: Daily Beast

Date: 23 Feb 2022

Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In

Ukrainian government websites were knocked offline Wednesday in a new wave of cyberattacks pummeling Ukraine, just as Russian forces are starting to roll into the country and Ukraine declares a nationwide state of emergency over Russia's recent aggression. The sites of Ukraine's Ministry of Foreign Affairs, its Security Service or SBU, and Cabinet of Ministers were all down Wednesday. Banks are also affected, Ukraine's minister of digital transformation, Mykhailo Fedorov, said on his Telegram channel. Ukrainian soldiers have also recently reported receiving alarming text messages urging them to flee or be killed, in what appeared to be an attempt to degrade their morale. Hackers have also recently deployed wiper malware, or destructive software, in Ukraine, cybersecurity researchers at ESET said Wednesday. READ MORE

RELATED ARTICLE:

The Washington Post, In the wake of the Ukraine invasion, Russia's cyberattacks could go global, 24 February 2022

BBC, Ukraine crisis: 'Wiper' discovered in latest cyber-attacks, 22 February 2022

Source: Infosecurity Magazine

Date: 25 Feb 2022

Anonymous Hacking Group Declares "Cyber War" Against Russia

"Hacktivist group Anonymous has declared 'cyber war' against Vladimir Putin's government following the Russian invasion of Ukraine. The well-known international hacking collective made the announcement on its Twitter account on Thursday, shortly after the Kremlin commenced military action. The message read: 'The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine.' Shortly after, the group claimed responsibility for taking down Russian government websites, including the Kremlin and State Duma. […] Cyber has already played a major role in the Russia-Ukrainian dispute over recent weeks, which has now spilled into armed conflict. Ukrainian government and critical services have been repeatedly hit with attacks believed to have been perpetrated by Russian cyber-criminals." READ MORE

RELATED ARTICLE:

The Guardian, Anonymous: the hacker collective that has declared cyberwar on Russia, 27 February 2022

Source: Infosecurity Magazine

Date: 23 Feb 2022

EU Deploys Cyber Response Unit to Ukraine

"The EU is deploying a newly formed Cyber Rapid-Response Team (CRRT) to Ukraine to help the country combat Russian threat actors as troops start pouring over the border. The Lithuanian Ministry of National Defence tweeted the news yesterday, revealing that the move came at the request of the Ukrainian government. Lithuania will be leading the coalition of six EU countries – which also includes Croatia, Poland, Estonia, Romania and the Netherlands – in order "to help Ukrainian institutions to cope with growing cyber-threats." READ MORE

RELATED ARTICLE:

Reuters, Six EU countries send experts to help Ukraine deal with cyber threats, 22 February 2022

Source: The Frontier Post

Date: 28 Feb 2022

The Ad Hoc Committee to Elaborate a UN Cybercrime Convention

The first negotiating session of the Ad Hoc Committee (AHC) to elaborate a UN cybercrime convention will convene February 28-March 11 at UN Headquarters in New York. This session will address the proposed scope, objectives, and structure for the convention as well as the mode of work for negotiations. READ MORE

RELATED ARTICLE:

US Department of State, Principal Deputy Assistant Secretary Walsh's Prepared Remarks at the Ad-Hoc Committee to Elaborate a UN Cybercrime Convention, 28 February 2022

United Nations, (1st meeting) First session, Ad hoc committee on Cybercrime (28 February-11 March 2022), 28 February 2022

Article 19, Proposed UN Cybercrime Convention must uphold free speech, 17 February 2022

Source: Lowy Institute

Date: 24 Feb 2022

The election for the future of the Internet

"In September this year, UN member states will cast their votes for the next secretary-general of the International Telecommunication Union (ITU). While elections for bureaucratic positions in obscure, technical UN bodies normally pass unnoticed, the ITU has emerged as the major battleground in Russia and China's fight for control of the internet. This election isn't just a vote for the next secretary-general, it's an election that will determine the future of cyberspace. […] Even with the internet, the ITU is just one part of the global ICT ecosystem with decisions over the technical governance of the internet taking place in other fora. Indeed, the multi-stakeholder approach to internet governance was deliberately created by the United States in the early days of the internet as a decentralised network so that nation states had limited control over the space." READ MORE

Source: Medianama

Date: 21 Feb 2022

Brazil joins the Convention on Cybercrime: How will it impact other BRICS countries?

"The Federal Senate of Brazil approved the draft legislative decree triggering Brazil's adhesion to the Convention on Cybercrime [...]. Despite its European genesis, the treaty ended up attracting the attention of non-European nations, becoming a global reference. Since 2001, 66 countries have ratified the Convention, including several large non-European countries such as Argentina, Canada, Japan, [...] and the United States. By providing consistency and a technology-neutral approach to cybercrime, the Convention plays a useful role in setting international standards on a key issue that, by definition, involves and affects actors in different jurisdictions." READ MORE

Source: Council of Europe

Date: 15 Feb 2022

Council of Europe & IAP: Spotlight on joint investigation teams and joint investigations on cybercrime and electronic evidence

"The fourth webinar in the series dedicated to the Second Additional Protocol (SAP) to the Budapest Convention, jointly organised by the International Association of Prosecutors (IAP) and the Council of Europe through the GLACY+ and the Octopus Project, took place on 15 February 2022. This webinar was focused on the new provisions regarding joint investigation teams and joint investigations on cybercrime and electronic evidence, as set forth in the Second Additional Protocol to the Budapest Convention. The experts provided insight, from both US and European perspective, on the new legal tools for joint investigations on cybercrime and electronic evidence with a view to achieve a better preparation of criminal justice authorities to implement the provisions of the Second Additional Protocol." READ MORE

Source: Sic Noticias

Date: 20 Feb 2022

Perguntas e respostas sobre ciberataques: quais os mais comuns, as intenções e haverá hackers bons e maus?

"No ano passado, o número de ciberataques realizados aumentou 50% a nível global em comparação a 2020. Apesar de a África, a Ásia e a América Latina aparecerem como os principais alvos, foi a Europa que registou o maior crescimento percentual de ciberataques (68%) [...]. No mesmo relatório, pode ler-se que os ataques de phishing e smishing (por SMS) continuam a dominar entre os incidentes registados. Apesar da designação complexa, estes ataques materializam-se através de e-mails ou mensagens enviadas para o telemóvel. O objetivo é obter acesso ao dispositivo ou conseguir dados pessoais e/ou credenciais (usernames e passwords). [...] Apesar das graves consequências, os ataques mais utilizados «são simples de executar do ponto de vista técnico» e «têm sempre um fator humano associado», explicou André Baptista, especialista em Cibersegurança." READ MORE

Source: Domain Name Wire

Date: 25 Feb 2022

ICANN: complaints and compliance

"How much of ICANN's time is spent dealing with compliance? The department enforces ICANN's contracts with registries and registrars. They handle complaints from registrants and end users, conduct audits, and monitor the domain name industry. [...] Every upheaval in the domain industry has impacted compliance activity within ICANN. Events in the domain space and community pressure typically result in increased compliance efforts. [...] GDPR, which has caused most Whois data to be redacted, has had a significant impact on complaints." READ MORE

Source: Business Daily Africa

Date: 24 Feb 2022

How legal loopholes are hurting Kenya's cybercrime fight

"Suits involving cybercrimes have been growing in recent years. Yet, only a handful end up in courts. Away from the glare of the public, Kenyan businesses are battling a silent, vicious and existential crisis of cybercriminals who either make illegal money transfers or encrypt data and demand ransoms running into hundreds of millions of shillings. «A significant number of companies and individuals are choosing to negotiate with cybercriminals in order to avoid any damage to their reputation and user trust that may be caused by a public trial», explains High Court advocate Peter Maina [...] Njoroge notes that poor handling of evidence in the chain of custody is a key challenge in cybercrime litigation. This often leads to its inadmissibility in court, he says." READ MORE

RELATED ARTICLE:

Engineering News, As ransomware attacks rise in Kenya, effective data backup becomes essential, 22 February 2022

Source: Business Live

Date: 18 Feb 2022

$3.5bn and growing: The huge cost of cybercrime in Africa

"As the continent's GDP reached $3.3-trillion in the past few years, so the cost of cybercrime climbed to $3.5bn, with Nigeria, Kenya and SA recording the largest losses. In fact, according to the SA Banking Risk Information Centre, SA loses $157m annually to cyberattacks. [...] Government leaders and cyber intelligence experts came together at the inaugural Cyber Intelligence Africa 2022, held in Johannesburg earlier this month, to discuss national cyber security strategies and policies, combating cybercrimes across Africa, international co-operation, threat intelligence and detection capabilities, and building cyber awareness. [..] 'As cybercrime becomes more advanced and scales, next-generation cyber intelligence solutions that identify, manage and respond to threats will be critical,' said Resecurity CEO Gene Yoo." READ MORE

Source: Council of Europe

Date: 23 Feb 2022

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

"The final meeting of the series of national workshops on the preparation of criminal justice statistics on cybercrime and e-evidence was held on the 23rd of February 2022 for the Moroccan authorities, within the framework of CyberSouth project. As in previous events of the series, the discussions covered different topics related to the relevance of statistics on cybercrime and e-evidence and the best practices on collecting and processing them. Representatives of judicial and law enforcement authorities presented their mechanism for collecting statistical data, followed by recommendations by the expert." READ MORE

RELATED ARTICLES:

Council of Europe, CyberSouth: National workshop on the preparation of criminal justice statistics on cybercrime and e-evidence in Algeria, 22 February 2022

Council of Europe, CyberSouth: National workshop on the preparation of criminal justice statistics on cybercrime and e-evidence in Jordan, 17 February 2022

Council of Europe, CyberSouth: National Workshop on the development of criminal justice statistics on cybercrime and e-evidence in Tunisia, 15 February 2022

Source: Daily News

Date: 27 Feb 2022

Tanzania: Govt touts cooperation in cybercrime fight

"The government has vowed to cooperate with other countries in fighting cyber crimes together with empowering its experts. The Permanent Secretary in the Ministry of, Communication and Information Technology, Dr Jim Yonazi made the remarks on Friday at the closing of five day training to police investigators and those in prosecution room on issues related to cybercrimes. Dr Yonazi said that issue of empowering experts to deal with cybercrime will go hand in hand with cooperation with other countries because cyber security issues are not limited to one country because the criminal can stay in another country and commit crimes in other countries." READ MORE

Source: Council of Europe

Date: 22 Feb 2022

GLACY+: Support for the Gambian legislative process on data protection

"In continuation of the support provided by the Council of Europe to the Gambian authorities in harmonising the data protection legal framework with the international standards and best practices, a validation workshop was organized on 22 February by the Council of Europe through the GLACY+ project and the Data Protection Unit. The Council of Europe's experts discussed with the Gambian counterparts [...] the recommendations and conclusions of the desk analysis [...]." READ MORE

Source: IOL

Date: 26 Feb 2022

Concern as South Africa features in top 10 list of countries hardest hit by cybercrime

"While South Africa sits sixth in the countries found to have the most cybercrime, research by the award-winning cybercrime company has shown that South Africa has shown the sharpest rise in cybercrime recently compared to any country in the world. [...] 'Using our breach detection mechanism, we found that in 2019 the number of breached users in South Africa has increased by a striking 490% compared to 2018,' Sablovskaja told the *Saturday Star* this week." READ MORE

Source: WakatSéra

Date: 25 Feb 2022

Burkina/Cybercriminalité: la Police alerte sur « une nouvelle forme d'arnaque »

"La Police burkinabè alerte les populations sur «une nouvelle forme d'arnaque», dans une note de la Brigade centrale de lutte contre la cybercriminalité diffusée le vendredi 25 février 2022. Selon la BCLCC, depuis quelques temps, plusieurs tenanciers de restaurants sont victimes d'une nouvelle forme d'arnaque appelée « arnaque sur le service traiteur»." READ MORE

Source: The National News

Date: 24 Feb 2022

Dubai-based Gems Education hit by cyber attack

"Gems Education, the largest education operator in the UAE, faced a cyber attack that had a minimal impact on the group's operations, the company said on Thursday. [...] Gems said it does not store the bank account details or credit card information of the families or guardians of its pupils. But it said some personal data could have been compromised. That includes identification documents, financial information, such as payment history, and data related to creditworthiness, health or medical records, and log-in details, such as usernames and passwords." READ MORE

Source: SeguriLatam

Date: 16 Feb 2022

México, a la cabeza en intentos de ciberataques en Latinoamérica y el Caribe

"México fue el país latinoamericano que más intentos de ciberataques (156.000 millones) recibió en 2021, seguido de Brasil (88.500 millones), Perú (11.500 millones) y Colombia (11.200 millones). [...] En el caso de la vulnerabilidad Log4J, que permitió la ejecución remota completa de código malicioso en sistemas vulnerables, los países latinoamericanos y caribeños que más intentos registraron fueron Perú, Colombia, Argentina, Brasil y México. En cuanto a los ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés), en el tercer trimestre de 2021 tuvo lugar el mayor ataque de este tipo de amenaza a través de una variante de la botnet Mirai dirigida a dispositivos IoT. Con unos 500.000 millones de intentos de ciberataques de DDoS, Brasil concentró el 10% del total. Igualmente, el año pasado se detectaron intentos de instalar herramientas de minería de criptomonedas en Argentina, República Dominicana y Colombia." READ MORE

Source: IT Sitio

Date: 24 Feb 2022

El malware Trickbot infecta más de 140.000 notebooks de clientes de Amazon, Microsoft y Google en Chile y el mundo

"Los ciberdelincuentes están atacando selectivamente objetivos de alto perfil para robar y comprometer sus datos confidenciales. Además, la infraestructura de este ciberataque puede ser utilizada por varias familias de malware para causar más daño en los equipos infectados. Check Point Research recomienda a los ciudadanos que solo abran documentos de fuentes de confianza, ya que los autores de Trickbot están aprovechando las técnicas de anti-análisis (que impiden o dificultan que el malware sea analizado) y anti-desfusión (dificultar la lectura de un código) para permanecer dentro de las unidades. El porcentaje de organizaciones afectadas por este troyano en cada región del mundo son altas. A nivel mundial. 1 de cada 45 empresas ha sido afectada, y en América Latina es 1 cada 42." READ MORE

Source: Telesemana

Date: 16 Feb 2022

Crecen las ciberamenazas en América latina y Brasil concentró el mayor ataque de denegación de servicio vía IoT

"El ojo de los ciberdelincuentes no sólo comienza a afinarse sino a sofisticarse en tiempos de acelerada transformación digital. Los ataques contra los usuarios finales han crecido un 600 por ciento en América latina en 2021 respecto a 2020. [...] En 2021, la región sufrió 289.000 millones de amenazas cibernéticas. Si hacemos un ejercicio para dimensionar cómo esto impacta en la vida de las personas y dividimos esta cantidad de ataques por la población de América latina y el Caribe, estimada en unos 667 millones de habitantes, el resultado es que cada una de las personas que viven en este suelo ha estado sometida a un promedio de 433 ataques en el año, o a más de uno por día. [...] El laboratorio también detectó una gran cantidad de ataques relacionados con la ejecución remota de código (RCE, por su sigla en inglés) en dispositivos IoT como cámaras, micrófonos y enrutadores domésticos" READ MORE

Source: ZD Net

Date: 24 Feb 2022

Asia most targeted region in 2021, taking on one in four cybersecurity attacks

"Asia was the most targeted region last year, accounting for one in four cybersecurity attacks launched worldwide. Japan, Australia, and India experienced the most incidents in the region, where server access and ransomware were amongst the most popular forms of attacks. Financial services and manufacturing organisations also bore the brunt of attacks in Asia, taking on almost 60% of such incidents, according to IBM's annual X-Force Threat Intelligence Index. [...] In Asia, server access attacks and ransomware were the top two forms of attacks last year, accounting for 20% and 11%, respectively, of all incidents. Data theft came in third at 10%, while remote access trojans and adware each accounted for 9% of attacks." READ MORE

Source: BBC

Date: 28 Feb 2022

Toyota to close Japanese factories after suspected cyber-attack

Toyota will shut down all 14 of its factories in Japan on Tuesday after a possible cyber-attack. News site Nikkei, which first reported the shutdown, said supplier Kojima Industries Corporation suspected it had been hit by a cyber-attack, causing a halt in production. Toyota is the world's best selling carmaker. Its production target for this year is 8.5 million vehicles. And the closure will reportedly set this back by about 13,000 cars. READ MORE

Source: Council of Europe

Date: 15 Feb 2022

GLACY+: Support for drafting data protection legislation in Vanuatu – Second workshop

"On 15 February 2022, the Council of Europe, through the GLACY+ Project and the Data Protection Unit, in collaboration with Vanuatu's National Task Force/Expert Group, organised the second workshop on data protection. The country's local authorities presented the Vanuatu's data protection, coordination and privacy concept note with a focus on the aim of the future Data Protection Policy. The Council of Europe's experts delivered presentations and led the dialogue on the international context of Vanuatu's development of a Data Protection Policy and Bill as well as on the way forward." READ MORE

Source: El Independiente

Date: 23 Feb 2022

Detienen a cinco ciberdelincuentes por robar 6 millones de euros a una empresa de criptomonedas

"La Guardia Civil ha desarticulado un grupo de ciberdelincuentes que en el verano de 2020 atacó una empresa española dedicada a la custodia de criptodivisas, materializando el robo de seis millones de euros en criptomonedas pertenecientes a miles de inversores, una operación que se ha saldado con cico detenidos y que se trata del primer caso de estas características resuelto en España. [...] La descarga ilegal de un disco pirata, el origen. Así, se pudo concluir que el mismo tenía su origen en la descarga ilegal de una película de un portal de contenido multimedia «pirata», por parte de un trabajador de la citada empresa. Los archivos que conformaban esa película contenían un virus informático altamente sofisticado que permitió a los atacantes hacerse con el control absoluto del ordenador del empleado y usarlo como cobertura para acceder a la empresa." READ MORE

Source: Rádio Renascença

Date: 18 Feb 2022

Casos de cibercrime duplicam a cada ano

"Os casos de cibercrime estão a aumentar à escala global e Portugal não é exceção.[...] «Nestes últimos dois anos houve um aumento brutal da cibercriminalidade. De 2019 para 2020 duplicou, mais do que duplicou, de acordo com os nossos indicadores, e de 2020 para 2021, de novo, outra vez, mais do que duplicou. » [...] «Os criminosos mudaram-se para o espaço cibernético, onde tudo é muito mais fácil, onde estão longe da vítima, onde podem expandir o seu negócio», diz Pedro Verdelho. O coordenador assinala que «o espaço cibernético permitiu, pela primeira vez na história do crime, globalizar o negócio, porque os criminosos estão sabe-se lá onde e atingem vítimas que nem eles sabem onde estão, em qualquer parte do mundo, em qualquer sítio»." READ MORE

RELATED ARTICLES:

Jornal de Notícias, Piratas informáticos ameaçam revelar informação da Impresa e Vodafone, 24 February 2022

Expresso das Ilhas, Especialista em cibersegurança alerta que ataques em Portugal podem ser replicados em Cabo Verde, 23 February 2022

Latest reports

- CISA, Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure, February 2022
- IBM Security X-Force Treat Intelligence Index 2022
- Tech Republic, Report: Pretty much every type of cyberattack increased in 2021, 17 February 2022
- Lexology, Cross-border data access: current state of play and outlook, 21 February 2022
- CompariTech, 300+ Terrifying Cybercrime and Cybersecurity Statistics (2022 EDITION), 22 February 2022
- ZD Net, Almost 100,000 new mobile banking Trojan strains detected in 2021, 22 February 2022
- IT Brief, Ransomware, threats, IoT malware, cryptojacking on the rise, 23 Febraury 2022
- ASPI, The future of assistance to law enforcement in an end-to-end encrypted world, 23 February 2022
- ENISA, CSIRT Maturity Framework - Updated and improved, 23 February 2022
- APWG, Phishing Activity Trends Report (4th Quarter 2021), 23 February 2022
- Security Brief, Ransomware attacks double in 2021, rise 93% - report, 24 February 2022
- Infobae, El secuestro de datos es el modo más común de ataques cibernéticos en Latinoamérica: cómo evitarlo, 24 February 2022
- ENISA, NFV Security in 5G - Challenges and Best Practices, 24 February 2022
- European Commission, 7th EU Internet Forum Ministerial: curbing harmful content online through joint efforts, 24 February 2022
- TintaTIC, Ransomware persistió como el ataque más común en América Latina en 2021, 25 February 2022
- Security Brief, Ransomware not slowing: Relentless and more destructive, 28 February 2022
- PplWare.Sapo, Saiba como começar a defender-se de Ciberataques, em 5 dicas úteis, 28 February 2022

Upcoming events

- 2 March, C-PROC/PHILIPPINES (online), Second roundtable on COVID-19-related cybercrime in the Philippines, OCTOPUS
- 2 March, C-PROC/ALGERIA, (*online*), National workshop on the development of a domestic toolkit for first responders to cybercrime investigations, CyberSouth
- 3 March, C-PROC/JORDAN, (*online*), National workshop on the development of a domestic toolkit for first responders to cybercrime investigations, CyberSouth
- 7 March, C-PROC/LATAM, (*online*), Series of regional webinars to Promote Universality and Implementation of the Budapest Convention on Cybercrime, GLACY+, OCTOPUS
- 7-9 March, C-PROC/ SRI LANKA, *(in person),* Regional Conference on cybercrime and COVID-19, GLACY+, OCTOPUS
- 7-11 March, C-PROC/GREECE, (*in person*), Regional Cyber Exercise (with Cybersecurity East project), CyberEast, iPROCEEDS-2
- 11 March, C-PROC/LATAM , (*online*), Participation in the XL Ordinary Meeting of FOPREL, GLACY+
- 15 March, C-PROC/UGANDA, (*hybrid*), Advisory workshop on harmonization of legislation on cybercrime and electronic evidence, GLACY+
- 15 March, C-PROC/MOROCCO, (*online*), National workshop on the development of a domestic toolkit for first responders to cybercrime investigations, CyberSouth
- 15 March, C-PROC/BOSNIA AND HERZEGOVINA, (*online*), Workshop on lawful interception of telecommunication traffic and access to retained data in line with EU regulations and ETSI standards, iPROCEEDS-2

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 March 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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime