Cybercrime Digest

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

1 – 15 August 2022

Source: Security Week

Date: 10 August 2022

Number of Ransomware Attacks on Industrial Orgs Drops Following Conti Shutdown

"The number of ransomware attacks on industrial organizations decreased from 158 in the first quarter of 2022 to 125 in the second quarter, and it may be — at least partially — a result of the Conti operation shutting down. According to data collected by industrial cybersecurity firm Dragos, Conti accounted for a significant chunk of the ransomware attacks on industrial organizations and infrastructure in the previous quarters and the threat actor's decision to pull the plug on the operation in May could have led to the drop in the number of attacks in the second quarter. Experts believe the Conti operation, which had been a highly profitable business, was shut down after the brand became toxic following some of the group's members openly expressing support for Russia after it launched its invasion of Ukraine." READ MORE

RELATED ARTICLE:

Help Net Security, A third of organizations experience a ransomware attack once a week, 4 August 2022

Source: timesofisrael.com

Date: 15 August 2022

3 arrested in Israeli probe of crypto scheme that defrauded the French government

"The Israel Police arrested three people Monday morning on suspicion of conducting a money-laundering service on behalf of criminals in France who defrauded the French government out of millions of euros. The suspects are believed to have used various cryptocurrencies to launder the money, and then return it as ostensibly "clean money" to the French fraudsters, the police said. It remains unclear exactly how the alleged money launderers in Israel were remunerated for their services." READ MORE

Source: Bleeping Computer

Date: 10 August 2022

Phishing attack abuses Microsoft Azure, Google Sites to steal crypto

"A new large-scale phishing campaign targeting Coinbase, MetaMask, Kraken, and Gemini users is abusing Google Sites and Microsoft Azure Web App to create fraudulent sites. These phishing pages are promoted through comments posted to legitimate sites by a network of bots controlled by the threat actors. Posting links to phishing pages on various legitimate sites aims to increase traffic and boost the malicious site's search engine rankings. Furthermore, because the phishing sites are hosted in Microsoft and Google services, they aren't flagged by automated moderator systems, allowing promotional messages to stay in the comment section for longer." READ MORE

Source: nftnow.com

Date: 10 August 2022

New EU Law Will Regulate NFT Collections Like Cryptocurrencies

"On August 2, during a panel at Korea Blockchain Week, European Union (EU) Advisor Peter Kerstens offered new insights into the EU's attempts to create broad regulatory measures in the crypto and NFT spaces. According to Kerstens, under the Markets in Crypto-Assets (MiCA) law, NFT collections will receive the same treatment as cryptocurrencies, CoinDesk reports. With this new classification, EU citizens hoping to put an NFT collection up for sale will fall under the umbrella of crypto-asset service providers (CASPs) and will need to receive express authorization from the EU before offering up their services (or wares) to the public. Via these measures, the EU hopes to "protect investors and preserve financial stability, while allowing innovation and fostering the attractiveness of the crypto-asset sector," according to a press release. This process is expected to take anywhere from one to three months, with larger CASPs subject to reports on their activities regularly submitted to the European Securities and Markets Authority (ESMA) by their local governments." READ MORE

Source: gub.uy

Date: 12 August 2022

Uruguay, Ministerio de Relaciones Exteriores: Visita Consejo de Europa por Convenio de Budapest sobre Ciberdelincuencia

"Por invitación del Ministerio de Relaciones Exteriores, una delegación del Comité del Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa realizó una visita de trabajo a Uruguay los días 11 y 12 de agosto. El Convenio de Budapest es el único tratado internacional que tiene por objetivo central el abordaje integral de la problemática de la ciberdelincuencia y cuenta actualmente con 66 Estados Parte y 15 Estados Observadores." READ MORE

Source: Argentina.gob.ar

Date: 10 August 2022

Se realizó la Primera Conferencia Cumbre sobre Asuntos Cibernéticos

"El titular de la Unidad Gabinete de Asesores (UGA) del Ministerio de Seguridad de la Nación, Lucas Gaincerain, y el director de Investigaciones de Ciberdelito, Pedro Janices, clausuraron la Primera Conferencia Cumbre sobre Asuntos Cibernéticos, que convocó a más de 36 oradores de organizaciones nacionales e internacionales, empresas de tecnología y funcionarios, para debatir sobre proyectos, experiencias, posibles soluciones y colaboraciones en temas como la cooperación internacional en prevención e investigación de ciberdelitos. […] Entre los oradores estuvieron representantes del Comité de la Convención sobre Cibercrimen del Consejo de Europa; del Instituto de Estudios de Seguridad de la Unión Europea; del proyecto EU Cybernet; de la Organización de Estados Americanos; de INTERPOL; del Global Forum on Cyber Expertise; del Operation Underground Railroad; y la embajadora para Asuntos Cibernéticos del Ministerio Federal de Relaciones Exteriores de Alemania." READ MORE

Source: ogdi.org

Date: 12 August 2022

Guatemala: Diputados presentan objeciones a la ley contra la ciberdelincuencia

"Debido a las críticas a la Ley contra la Ciberdelincuencia aprobada por los diputados el pasado 4 de agosto. Congresistas del Grupo Parlamentario de Oposición, presentaron un documento con objeciones al decreto 39-2022. Según el diputado Carlos Barreda, es necesario archivar la ley porque la misma quiere castigar las voces opositoras. "El objetivo es que el día martes de la próxima semana, cuando la Junta Directiva convoque al pleno se tenga que conocer las observaciones y las objeciones al decreto 39, Ley de Prevención y Protección contra la Ciberdelincuencia, la intención es que esta ley se archive y se discuta a profundidad, porque se quiere aprovechar el tema de la ciberdelincuencia para reprimir la oposición política y callar a la prensa", dijo el congresista." READ MORE

Source: es us.finanzas

Date: 12 August 2022

Dónde se ubica México en temas de ciberseguridad mundial

"Mexico fue el cuarto país más atacado (de 17), según el estudio, con 90.6% de las empresas habiendo sido víctimas al menos de un ataque exitoso en el último año; 40% del total de las compañías contenidas en el estudio declaran haber tenido más de 6 ataques exitosos en el año. […] En el tema de la negación, lo alarmante es que en el mundo 76% de las empresas creen que en los próximos 12 meses un ataque exitoso es muy probable que suceda (cuando el año pasado atacaron a 85% de ellas; 9 puntos de diferencia) el número más alto desde que el estudio se fundó en 2014." READ MORE

Source: zawya.com

Date: 3 August 2022

ECOWAS strengthens capacity of Cybercrime First Responders

"The ECOWAS Commission within the framework of the Organised Crime: West African Response on Cybersecurity and fight against Cybercrime" (OCWAR-C) project and in collaboration with the Council of Europe and INTERPOL held an E-Evidence and First Responders Training of Trainers workshop in Praia, Cabo Verde from 25 – 29 July 2022. The reliance on information communication technology is more pervasive in society, with an increased use in personal devices across the region. This has necessitated the need for law enforcement' entities to develop the required capacities to ensure efficient investigation and handling of digital evidence is carried out to appropriate standards." READ MORE

RELATED ARTICLES:

Modern Ghana, ECOWAS builds the capacity of law enforcement entities, 9 August 2022

AfriMag, Cybercriminalité en Afrique de l'Ouest : La CEDEAO renforce les capacités des formateurs sur la preuve électronique, 11 August 2022

Source: cio-mag.com

Date: 4 August 2022

Cybersécurité: la démarche inclusive pour le Togo

"Le Conseil des ministres a recommandé, mercredi 3 août, une synergie d'action entre les acteurs de la cybersécurité au Togo. Cet appel s'inscrit dans la vision de mutualisation des efforts que prônent les autorités togolaises. Les acteurs du public, du privé et l'Agence nationale de la cybersécurité (ANCy) sont invités à collaborer ensemble pour une meilleure sécurisation du cyberespace togolais. Le gouvernement a fait cette recommandation suite à une communication de la ministre Cina Lawson en charge de l'économie numérique et de la transformation digitale, mercredi en Conseil des ministres. La ministre a présenté au gouvernement l'état de l'écosystème de la cybersécurité, depuis la création de l'ANCy et son bras opérationnel Cyber Defense Africa." READ MORE

Source: cybersecuritymag.africa

Date: 8 August 2022

Sextorsion au Bénin: l'Office de répression de la cybercriminalité alerte sur un nouveau mode opératoire

"L'Office central de répression de la cybercriminalité (OCRC) alerte sur un nouveau mode de sextorsion au Bénin et invite les populations à la vigilance. L'alerte a été donné le dimanche 7 août 2022 à travers une publication sur Facebook. « Il nous a été remonté plusieurs nouveaux cas de sextorsion avec un mode opératoire différent », alerte l'Office. Selon le détail donné par l'OCRC sur le nouveau mode opératoire, « les cybercriminels lancent des appels vidéo aléatoires » afin de faire de capture de visage. Ensuite, ils font un montage vidéo avec le visage de la victime et une autre vidéo la mettant dans une situation intime. Cela, indique l'Office, « dans le but de faire pression et d'extorquer de l'argent à cette dernière. Au regard du nouveau mode opératoire, l'Office central de répression de la cybercriminalité au Bénin invite les populations à éviter de décrocher des appels vidéo d'inconnus. « Contactez les autorités compétentes lorsque vous êtes victime », a conseillé l'Office invitant à la vigilance." READ MORE

Source: wazaa.mu

Date: 15 August 2022

Maurice : Exploitation d'enfants en ligne - renforcement des capacités à travers les projets GLACY+ et OCTOPUS

"Maurice redouble d'efforts dans le combat contre les phénomènes de pédopornographie et autres types d'exploitation d'enfants en ligne. Il s'agit d'une initiative de l'Union Européenne (UE) dont le but est de former les principaux acteurs qui agissent pour la protection et le bien-être des mineurs. Outre les sessions de formations, le renforcement des capacités fait également partie du programme qui découle de deux projets appelés GLACY+ et OCTOPUS. Notons que GLACY est l'acronyme de l'Action Globale sur la Cybercriminalité. Le projet est une collaboration entre l'UE et le Conseil de l'Europe. Il vise à soutenir les pays à l'échelle mondiale dans la mise en œuvre de la Convention sur la Cybercriminalité." READ MORE

Source: uniquenewsonline.com

Date: 5 August 2022

UAE: A New Cybercrime Legislation Makes it illegal to Photograph Someone in a Public Area

"The punishment for taking pictures of accident victims and disseminating them online has been changed under the new UAE cybercrime legislation. The legislation, which took effect on January 2, 2022, penalizes anyone who photographs others without their consent. Both offences are punishable by a six-month prison sentence or a fine ranging from Dh150,000 to 500,000, or both, under the modified UAE Cybercrime Law. The new federal legislation No. 34 of 2021 amended federal law no. 5 of 2012, which oversees Cybercrime and includes internet offences. The legislation aims to safeguard the public from online crimes committed via social media networks and information technology platforms and secure government websites and databases and prevent the spread of rumours and false or misleading information." READ MORE

Source: The Diplomat

Date: 4 August 2022

The Philippine-US Alliance Has a Major Blind Spot: Cybersecurity

"From imperial Japan to Communist insurgents and Islamic terrorists, the Philippine-U.S. defense relationship has effectively evolved over its 70-year lifespan to meet the changing regional and global threat environment. However, over the past 20 years, this adaptation has faltered. During this period, cyber operations have become an increasingly prominent tool of international conflict. Whereas other security partnerships like the North Atlantic Treaty Organization (NATO) and the Japan-U.S. alliance have undertaken significant measures to enhance collective defense in cyberspace, cyber cooperation has lagged within the Philippines-U.S. alliance. A functional alliance should be capable of not only preempting large-scale disruptive attacks, but also rebuffing sustained cyber campaigns that degrade institutional trust and shape strategic outcomes." READ MORE

Source: pjsp.govt.nz

Date: 5 August 2022

Council of Europe and PILON Cybercrime Working Group: Webinar - Cybercrime Legislation in the Pacific

"The webinar will discuss recent progress in harmonising and updating legal frameworks on cybercrime and electronic evidence, in line with international standards (i.e., Budapest Convention) as a crucial milestone in equipping relevant authorities in the region to address cybercrime issues. The webinar will offer Pacific countries the opportunity to share the approach their country has taken and discuss the merits of solutions to further strengthen the criminal justice response in the region." READ MORE

Source: 9news.com.au

Date: 13 August 2022

Google fined $60 million for misleading Australian Android users

"Google has been fined $60 million for misleading Australian Android users about how it used their location data. The internet giant was taken to court by the Australian Competition and Consumer Commission (ACCC) in 2019, who alleged that Android phone settings were misleading. The ACCC accused Google of keeping the location data of some users even if they had "Location History" turned off." READ MORE

Source: The Courier

Date: 9 August 2022

UK: Rising number of self-generated child sexual abuse images online reported

"Nearly 20,000 webpages of child sexual abuse imagery found in the first half of this year included self-generated content of children aged between seven and 10 years old, the Internet Watch Foundation (IWF) has said. The online safety group said the scale of content showing young children who had been coerced into creating imagery made it a social and digital emergency. The UK-based IWF is Europe's largest hotline dedicated to finding and removing images and videos of child sexual abuse online and said this year's figures were up nearly 8,000 on the same period last year and more than quadruple the number of images of this type found in the first half of 2020. IWF chief executive, Susie Hargreaves, said "more needs to be done" to combat the issue and called on the Government, tech companies and the police to work together more closely. "There is no place for child sexual abuse on the internet and we cannot simply accept, year on year, that sexual imagery of children is allowed to be exchanged without constraint online," she said." READ MORE

Source: therecord.media

Date: 11 August 2022

Pro-Kremlin hackers target Latvia's parliament after declaring Russia a sponsor of terrorism

"The pro-Russian hacker gang known as Killnet took down the website of Latvia's parliament on Thursday after lawmakers there designated Russia as a "state sponsor of terrorism." The parliament's website went down for several hours after being hit by a distributed denial-of-service (DDoS) attack, which floods websites with junk traffic to make them unreachable. The attack didn't disturb the work of the parliament, known as the Saeima, "due to previously prepared defence solutions," according to Latvia's Computer Emergency Response Team (CERT.LV). Killnet wrote about the attack on its official Telegram channel and posted a screenshot confirming that the website was down." READ MORE

Source: arstechnica

Date: 5 August 2022

Cyberattack on Albanian government suggests new Iranian aggression

"In mid-July, a cyberattack on the Albanian government knocked out state websites and public services for hours. With Russia's war raging in Ukraine, the Kremlin might seem like the likeliest suspect. But research published on Thursday by the threat intelligence firm Mandiant attributes the attack to Iran. And while Tehran's espionage operations and digital meddling have shown up all over the world, Mandiant researchers say that a disruptive attack from Iran on a NATO member is a noteworthy escalation. The digital attacks targeting Albania on July 17 came ahead of the "World Summit of Free Iran," a conference scheduled to convene in the town of Manëz in western Albania on July 23 and 24. The summit was affiliated with the Iranian opposition group Mujahadeen-e-Khalq, or the People's Mojahedin Organization of Iran (often abbreviated MEK, PMOI, or MKO). The conference was postponed the day before it was set to begin because of reported, unspecified "terrorist" threats." READ MORE

Source: lebigdata.fr

Date: 9 August 2022

Cyberattaque massive aux portes de la France, l'Allemagne frappée

"Une cyberattaque massive frappe l'Association des chambres du commerce et de l'industrie en Allemagne (DIHK). Les responsables informatiques ont été contraints de mettre hors ligne l'ensemble des réseaux : les services numériques, les téléphones, les serveurs de messagerie. Les responsables qualifient l'incident de « massif »." READ MORE

RELATED ARTICLE:

Therecord.media, Massive' cyberattack hits German Chambers of Industry and Commerce, 5 August 2022

Latest reports

- The Europol Podcast, Episode 1: Protecting vulnerable children, 1 August 2022
- Microsoft, Cyberthreat Minute: The scale and scope of worldwide cybercrime in 60 seconds, 1 August 2022
- Estrategia y Negocios, Lo que las empresas deben saber ante aumento de ciberataques, 3 August 2022
- L'Echo, Cybercriminalité : toujours plus d'infractions en Belgique, 4 August 2022
- World Economic Forum, How to align cyber risk management with your business needs | World Economic Forum (weforum.org), 4 August 2022
- Ropes & Gray, Further EU and UK Developments in Financial Crime Regulation of Crypto assets, 4 August 2022
- Cybernews, Cybercrime in 2023: ransomware, LockBit, and emerging hacktivism, 5 August 2022
- Talos Intelligence, Small-time cybercrime is about to explode — We aren't ready, 8 August 2022
- Eurojust, Report on Eurojust's casework in the field of the European Investigation Order, 8 August 2022
- Africa cybersecurity magazine, Rapport KnowBe4 et IDC : la cybersécurité en Afrique subsaharienne, 8 August 2022
- Avira Protection Labs, Avira Cyber Threat Report, 10 August 2022
- Embroker, 2022 Must-Know Cyber Attack Statistics and Trends, 12 August 2022
- Cyber Edge Group, Cyberthreat Edge Report, August 2022

Upcoming events

- 15-31 August, C-PROC, Further development of the cyberviolence resource, Octopus
- 16-19 August, C-PROC/BENIN, *(hybrid),* Support the national delivery of the Introductory Course on cybercrime and electronic evidence for Judges and prosecutors, Part 1 (ToT), GLACY+ with OCWAR-C
- 18-19 August, C-PROC/PORTUGAL/ROMANIA*, (hybrid),* Pilot workshop on the implementation of the 2nd Additional Protocol in domestic legislation, Octopus
- 19-21 August, C-PROC/ SRI LANKA, *(online),* Refresher on the Budapest Convention, on Cybercrime and on electronic evidence for Trainer Justices of Supreme Court of Sri Lanka and courts of appeal, 2/2 (High Court Judges), GLACY+
- 22-25 August, C-PROC/ PERU, *(in-person)*, Initial assessment, GLACY+
- 26 August, T-CY, *(online),* 8th Meeting of the Working Group on Undercover Investigations and extension of searches
- 29 August-9 September, CPROC, *(in-person)*, Support the participation of delegates from a selected number of countries to the Ad Hoc Committee on new UN Treaty, third meeting, GLACY+ and Octopus
- 29 August-2 September, CPROC/UKRAINE, *(online),* OSINT Training for Prosecutors Training Center of UA, CyberEast
- 30 August-2 September, CPROC/BENIN, *(hybrid),* Support the national delivery of the Introductory Course on cybercrime and electronic evidence for Judges and prosecutors, Part 2, GLACY+ with OCWAR-C
- 31 August-2 September, C-PROC/SOUTH KOREA, *(in-person),* International Symposium on Cybercrime Response, South Korea, Octopus

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