Cybercrime Digest

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

01 – 15 June 2024

Source: Council of Europe

Date: 01 June 2024

The Council of Europe works to create a safer digital environment for children worldwide

"On the occasion of 1 June, which marks the International Day for the Protection of Children in several countries around the world, the Council of Europe reiterates its commitment to protect children's rights and wellbeing, online and offline, through relevant treaties and effective mechanisms that function in synergy. […] While the Lanzarote Convention sets the ground for criminalising sexual abuse and exploitation offences, the Convention on Cybercrime provides the relevant procedural framework for criminal investigations, the collection of electronic evidence and the facilitation of cross-border cooperation. The Convention is supplemented by the Second Additional Protocol on enhanced international co-operation and disclosure of electronic evidence […]." READ MORE

Source: European Commission

Date: 13 June 2024

EU law on combatting violence against women enters into force

"Today, the first ever EU rules on combating violence against women and domestic violence enter into force. Violence against women and domestic violence affect an estimated one in three of the 228 million women in the EU. […] The new rules are decisive against gender-based violence, and ban female genital mutilation, forced marriage and the most widespread forms of cyber violence, such as the non-consensual sharing of intimate images (including deepfakes), cyber stalking and cyber harassment (including cyber flashing). Cyber violence is an urgent issue to address, given the exponential spread and dramatic impact of violence online." READ MORE

Source: Eurojust

Date: 14 June 2024

Major takedown of critical online infrastructure to disrupt terrorist communications and propaganda

"Judicial and law enforcement authorities across Europe and in the United States have dismantled critical online infrastructure in a large-scale operation to disrupt platforms and websites for terrorist communications and propaganda. In a concerted major action this week, servers were taken down in Germany, the Netherlands, United States and Iceland, with the Spanish authorities arresting nine radicalised individuals. The servers supported multiple media outlets linked to Islamic State. They were used to disseminate worldwide propaganda and messages capable of inciting terrorism in at least thirty languages. Eurojust and Europol coordinated and supported the joint operations." READ MORE

RELATED ARTICLE:

Europol, Europol-coordinated operation tackles the threat of terrorist-operated websites, 14 June 2024

Source: Sage Journals

Date: 06 June 2024

Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation

"As the 'cyber' element infiltrates a significant part of criminal activity, the significance of accessing electronic evidence has risen to a critical level. The storage of this evidence outside the investigating jurisdiction prompted law enforcement authorities to actively explore avenues for collaboration with private service providers on a voluntary basis. This has resulted in the establishment of an informal channel of cooperation, running parallel to those established through mutual legal assistance and the principle of mutual recognition. The EU legislator has recently formalised this type of cooperation by adopting the Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence, along with the Directive (EU) 2023/1544." READ MORE

Source: Ciso

Date: 15 June 2024

ICC probes cyberattack in Ukraine as possible war crimes, sources say

"The International Criminal Court is investigating alleged Russian cyberattacks on Ukrainian civilian infrastructure as possible war crimes. This marks the first investigation of attacks in cyberspace by international prosecutors, potentially leading to arrest warrants if enough evidence is gathered. […] The probe is examining attacks on infrastructure that endangered lives by disrupting power and water supplies, cutting connections to emergency responders or knocking out mobile data services that transmit air raid warnings, […]." READ MORE

Source: The Week

Date: 03 June 2024

How the FBI took down the world's largest zombie 'botnet'. The bot allegedly infected more than 19 million IP addresses across the world

"The United States is taking a major victory lap after federal authorities took down what was allegedly the largest zombie "botnet" in the world. A Chinese national, YunHe Wang, was arrested as the mastermind of 911 S5, a proxy bot service that was «used to commit cyber attacks, large-scale fraud, child exploitation, harassment, bomb threats and export violations,» the U.S. Department of Justice (DOJ) said in a press release. […] The so-called «zombie» botnet was a system that deployed malware onto various computers, and was designed to infect as many devices as possible. […] Altogether, Wang reportedly «made more than $99 million selling cybercriminals access to his hijacked devices» […]. He would then use the funds to purchase luxury vehicles, real estate, watches and other high-end goods." READ MORE

RELATED ARTICLE:

FBI, Inside the FBI: The 911 S5 Cyber Threat, 07 June 2024

Source: Radio Fides

Date: 13 June 2024

Alerta en Latam: Más del 40% de los usuarios de internet está expuesto a los ataques de hackers por mirar fútbol libre pirata

"El 8 de junio se celebró el Día Mundial Contra la Falsificación y la Piratería. Más de 40 millones de hogares en Latinoamérica acceden a sitios clandestinos que promocionan la transmisión gratuita de partidos. Los sistemas piratas ingresan a los celulares, tabletas y computadoras de los usuarios y les roban datos bancarios y de tarjetas de crédito, además de sus datos y archivos personales." READ MORE

Source: Asamblea Nacional, Ecuador

Date: 14 June 2024

Ecuador: Convenio de Budapest sobre la ciberdelincuencia se analizó en la comisión de seguridad integral

"Para la presidenta de la comisión, Inés Alarcón, el texto aborda el combate a los delitos informáticos y es la normativa más completa, a nivel mundial, en esta materia. Paola Falconí, delegada de Relaciones Exteriores, coincidió con la legisladora al mencionar que «este instrumento internacional busca prevenir el crecimiento de la ciberdelincuencia en países que no cuentan con la legislación adecuada para tipificar los ciberdelitos»." READ MORE

RELATED ARTICLE:

Global Support, Necesidad de aprobación legislativa del Convenio de Budapest, 11 June 2024

Source: El Informante

Date: 11 June 2024

México no tiene capacidad para combatir ciberdelitos

"México es un país de contrastes en lo que a ciberseguridad se refiere, ya que si bien se encuentra entre los mejor capacitados de América Latina para enfrentar amenazas en el ciberespacio, tiene la tasa más alta de ciberdelitos en la región. Un grupo de analistas coinciden en señalar que es la falta de leyes en la materia, la poca inversión en sus capacidades cibernéticas y la ausencia de educación y de habilidades para generar una cultura de la ciberseguridad, lo que propicia que el país esté en dicho estancamiento." READ MORE

Source: El Diario

Date: 02 June 2024

Bolivia: Tres causas por las que no se denuncian ciberdelitos

"«Primero es la vergüenza de las personas a quienes le ocurren; segundo, desconfianza en las autoridades de administración de justicia, Policía, Fiscalía y juzgados; el tercero, es un desconocimiento por parte de las personas en temas de ciberseguridad y protección de datos personales para resguardar su información adecuadamente», detalló el especialista a Unitel. […] Agregó que el modus operandi de estas organizaciones es a través de múltiples delitos comunes y corrientes, tales como estafa, falsificaciones o extorsiones. Una vez que tienen la información, proceden a extorsionar o afectar a la persona de alguna manera." READ MORE

Source: Cambio

Date: 11 June 2024

Colombia es el país más afectado por ataques cibernéticos en América Latina

"El ataque cibernético de Emcali, ocurrido el pasado 9 de junio, se suma a los más de 20,000 millones de ciberataques que reportó el ministro de las TIC, una cifra significativa en comparación con los 12.000 casos que se habían registrado en 2023. Aunque el gerente general de la empresa, Roger Mina, aseguró a los medios de comunicación que la situación fue contenida en menos de dos horas, este caso se suma a las más de 3.147 denuncias por ataques cibernéticos que se han reportado en los últimos meses, según datos de la Policía Nacional. En lo corrido del año se han reportado más de 20.000 millones de ciberataques según el ministro de las TIC, Mauricio Lizcano, quien compartió los datos y avances de la estrategia Colombia PotencIA Digital con los asistentes a la Convención Bancaria 2024." READ MORE

RELATED ARTICLE:

Redcómputo, En 2023, Colombia reportó 28.000 millones de ciberataques financieros, 05 June 2024

Source: Netskope

Date: 13 June 2024

Two Recent Campaigns from Brazil and Korea Exploiting Legitimate Cloud Services

"Two recent examples bring us to Brazil and Korea, where two distinct operations provided additional, unneeded, proofs of how legitimate internet services can be easily adapted for multiple roles and multiple purposes over the course of a malicious operation. In May, researchers at HarfangLab in Brazil discovered a malicious campaign delivering a payload named "AllaSenha" (yet another variant of an old acquaintance for users in Latin america: AllaKore, an open source remote access tool). […] Nearly at the same time, researchers at AhnLab found out that cybercriminals were quite busy in South Korea, distributing a malware cocktail (remote access Trojans, cryptocurrency miners, malware downloaders, proxy tools, and anti-AV programs) through cracked versions of Microsoft Office (once again a warning to not install unapproved applications on corporate devices)." READ MORE

Source: Forbes Argentina

Date: 04 June 2024

Ciberataques en Argentina: se registraron 262 millones de intentos de intrusión en el primer trimestre

"La Argentina registró más de 262 millones de intentos de ciberataques durante el primer trimestre de este año, con enero y marzo como los meses de mayor actividad. Este dato se desprende del informe del panorama de amenazas presentado por Fortinet. […] «En todos los sensores de Fortinet, las detecciones de ransomware cayeron un 70% en comparación con el primer semestre de 2023. La desaceleración observada en el ransomware durante el último año se puede atribuir a que los atacantes pasan de la estrategia tradicional de 'distribución y oración' a una estrategia mucho más focalizada, dirigida en gran medida a las industrias de energía, atención médica, manufactura, transporte y logística, y automotriz», destacaron desde la firma, […]." READ MORE

Source: African Manager

Date: 07 June 2024

Tunisie: L'ARP écoute la partie initiatrice du projet de loi sur la cybersécurité

"Selon le représentant de la partie initiatrice, la ratification par la Tunisie de la convention du Conseil de l'Europe sur la cybercriminalité, ouverte à la signature le 23 novembre 2001 à Budapest, et l'ampleur du phénomène des cyberattaques, exigent de la Tunisie de promulguer un texte de loi. Il a ajouté que la protection des institutions nationales stratégiques à l'instar de la Banque centrale et de l'Instance nationale de protection des données personnelles des cyberattaques constitue une priorité qui doit être élevé au rang de la sécurité nationale." READ MORE

Source: Council of Europe

Date: 05-06 June 2024

CyberSouth+ Workshop on Standard Operating Procedures with Lebanon

"The CyberSouth+ project organized a two-day workshop, on-line, with representatives from the Lebanese Internal Security Force (ISF) and judiciary on Standard Operating Procedures (SOPs) in cybercrime cases and electronic evidence. The aim of the event was to discuss with Lebanese stakeholders the use of the SOPs developed with the support of the previous project CyberSouth (2017-2023), assess their validity as well as amendments and/or integration to cover all procedural aspects." READ MORE

Source: Council of Europe

Date: 12-13 June 2024

CyberSouth+: National guide on cybercrime and electronic evidence

"The joint EU/CoE CyberSouth+ project paid an official visit to Algeria to discuss the development of a judicial national guide on cybercrime and electronic evidence and the support to the personal data protection regime, recently introduced by the country. Following up on previous activities carried out by the project, Algeria requested the CyberSouth+ project team to assist with the implementation of the recently adopted legislation on personal data protection, with reference to data used for criminal investigations, judicial decisions and international co-operation, also in light of the operational agreement currently under discussion with EUROJUST." READ MORE

Source: Council of Europe

Date: 06-08 June 2024

CyberSouth+ Basic judicial training course on cybercrime and electronic evidence for magistrates

"The CyberSouth+ project assisted the High Institutes for Magistrates of Morocco in organising a basic judicial training course on cybercrime and electronic evidence in Tangier, from 6 to 8 June 2024, enabling forty in service magistrates to acquire new skills and knowledge to fulfil their roles and functions in cases involving cybercrime and electronic evidence.[…] The project will continue working with the Moroccan judiciary and next activities will be organized with the General Prosecution Office in October 2024 to enhance capacity of reference magistrates in decentralized jurisdictions." READ MORE

Source: We are Tech Africa

Date: 14 June 2024

Le Niger durcit sa loi sur la cybercriminalité

"Selon le ministère chargé de la Justice, cette modification a pour objectif de « rétablir l'équilibre entre la liberté d'expression et la protection des droits individuels et de préserver la tranquillité et la sécurité publique ». Désormais, la diffusion de contenus troublant l'ordre public ou portant atteinte à la dignité humaine est punie d'une peine d'emprisonnement de deux à cinq ans et d'une amende de deux à cinq millions de francs CFA (soit environ 3 000 à 7 600 euros). La diffamation et les injures proférées par voie électronique sont quant à elles punies d'un an à trois ans de prison et d'une amende d'un à cinq millions de francs CFA." READ MORE

Source: Tech Afrika

Date: 07 June 2024

Un avocat nigérian critiqué pour sa défense générée par l'IA

"Dans une controverse juridique sans précédent, un avocat nigérian s'est retrouvé au centre d'une grosse polémique après avoir utilisé une défense générée par l'Intelligence Artificielle (IA) pour son client. […] Après un examen plus approfondi, il a été révélé que l'avocat avait utilisé un outil d'IA avancé pour générer la défense. Cet outil, conçu pour aider les professionnels du droit en générant des documents, en résumant les affaires et même en prédisant les résultats judiciaires, avait façonné toute la stratégie de défense." READ MORE

Source: Africa News

Date: 10 June 2024

Zambie: 22 Chinois et un Camerounais inculpés pour cybercriminalité

"Un tribunal zambien a condamné vendredi 22 ressortissants chinois à des peines d'emprisonnement pour des actes de cybercriminalité, notamment des fraudes et des escroqueries en ligne visant des Zambiens et d'autres personnes de Singapour, du Pérou et des Émirats arabes unis. […] L'entreprise, nommée Golden Top Support Services, avait employé des Zambiens « peu méfiants » âgés de 20 à 25 ans pour utiliser les cartes SIM afin d'engager « des conversations trompeuses avec des utilisateurs de téléphones portables peu méfiants sur diverses plates-formes telles que WhatsApp, Telegram, des salons de discussion et autres, en utilisant des dialogues scénarisés », a déclaré M. Banda en avril après le raid." READ MORE

Source: Sokong

Date: 10 June 2024

Cybercrime in Malaysia: An Epidemic?

"With social media rampant even among the elderly, opportunities for scammers are abundant. Often caught off-guard, the elderly leak personal information that scammers can exploit. The alarming rise in cybercrime in Malaysia calls for heightened awareness and precautionary measures, especially among the elderly, who are most at risk. As scams continue to evolve, staying informed and sceptical of unsolicited offers is crucial in protecting oneself from financial ruin. […] «Scammers often create complex structures to confuse and rush victims into making hasty decisions. It's essential to verify the legitimacy of investment offers by checking the licences of fund managers and agents through official channels […]»" READ MORE

Source: Elblog

Date: 03 June 2024

Unemployed Japanese Man Arrested for AI-Generated Malware Creation

"In a groundbreaking cybersecurity incident, an unemployed 25-year old from Kawasaki, Japan, has been taken into custody by law enforcement for allegedly crafting a virus using AI technologies available on the internet. This arrest marks a novel event where interactive generative artificial intelligence systems have been utilized in the development of malicious software. […] This case reflects the growing challenges and complexities in cybercrime, as AI tools become more widely accessible and potent. It underscores a potential trend where traditional cybersecurity measures may need to adapt to the emerging threats posed by the combination of AI technologies and cybercriminal activities." READ MORE

Source: Council of Europe

Date: 13-14 June 2024

GLACY-e: Support for the national conference on cybercrime for prosecutors

"Addressing cybercrime has become a strategic priority for most of Pacific countries. Several countries in the region have adopted domestic legislation and have taken meaningful steps towards the adhesion to the Convention on Cybercrime (Budapest Convention).[…] In his keynote speech, the Hon.Minister for Lands and Mineral Resources, highlighted that, «this conference is a significant step towards enhancing our collective capacity to combat cybercrime. Let us use this platform to engage in meaningful dialogue, share insights, and strengthen our resolve to protect our digital future.»" READ MORE

Source: Sangfor

Date: 04 June 2024

Australia: 500 Million+ Customers Affected by Ticketmaster Hack

"The entertainment industry in particular is known to collect and process multitudes of personal and private information that can be easily leveraged in phishing attacks on a larger scale. […] On the 29th of May, a hacking group by the name of ShinyHunters shared on a dark web forum that it had access to the data of 560 million Ticketmaster customers – amounting to almost 1.3 terabytes. The group was putting the data up for sale for a one-time price of US$ 500,000 and demanded that Ticketmaster pay a ransom to avoid the release of the information. According to the sample data posted by the group, the stolen information consists of customer names, addresses, phone numbers, and email addresses. It also included hashed credit card numbers, the last four digits of credit cards, credit card expiration dates, and fraud details. as well as customer names, addresses, and emails." READ MORE

Source: Attorney-General's Department

Date: 05 June 2024

Australia: New criminal laws to combat sexually explicit deepfakes

"The Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 will impose serious criminal penalties on those who share sexually explicit material without consent. This includes material that is digitally created using artificial intelligence or other technology. Digitally created and altered sexually explicit material that is shared without consent is a damaging and deeply distressing form of abuse." READ MORE

Source: Council of Europe

Date: 05-06 June 2024

CyberSEE and Octopus Project – CYBERKOP Action: EUROPOL AP Twins Annual Expert Meeting on Protecting Children Against Sexual Exploitation and Abuse

"The event covered a range of topics, including the impact of artificial intelligence and virtual reality on child protection. It provided a chance to discuss safeguarding children both online and offline, and to explore innovative solutions to overcome these issues. At the same time, the meeting facilitated sharing of insights on preventive measures, legal frameworks and strategic approaches for law enforcement and judicial authorities, being a platform for networking, collaboration and learning." READ MORE

Source: Intellinews

Date: 13 June 2024

Russian cyberwar against Ukraine and the West

"For years Russian hackers reportedly associated with the country's secret services have conducted numerous attacks against Western targets. But since Russia's invasion of Ukraine in February 2022 these attacks have stepped up, hitting targets in Ukraine, as well as its Western allies." READ MORE

RELATED ARTICLE:

U.S. Naval Institute, The Changing Character of Cyber Warfare, June 2024

Source: Council of Europe

Date: 04-06 June 2024

CyberSEE and Octopus Project – CYBERKOP Action: ISS World Training seminars for Law Enforcement, Financial Investigators and Cybersecurity Communities fighting against criminal activities over the Internet

"The event offered a variety of seminars and training sessions compiled into eight thematic tracks, covering tools, methodologies and equipment to enable law enforcement and intelligence communities to better tackle the challenges posed by the latest threats in cybercrime, cryptocurrencies, money laundering, artificial intelligence, darknet and other criminal activities conducted over telecommunications networks, the internet and social media." READ MORE

Source: RTS

Date: 06 June 2024

Première en Suisse présentée à Fribourg en matière de "e-justice"

"Fribourg présente une première en Suisse en lien avec son programme de "e-Justice". Avec la mise en oeuvre de ProofBox, solution dévoilée mercredi à Granges-Paccot, le canton franchit une nouvelle étape vers la numérisation de la justice, en suscitant un vif intérêt. […] Dans le paysage juridique actuel, la prédominance des preuves numériques dans les affaires pénales est devenue incontournable, ont dit les intervenants. Avec la multiplication des technologies numériques et l'omniprésence des appareils électroniques, les preuves sous forme électronique jouent un rôle "crucial" dans l'établissement des faits et la poursuite des enquêtes pénales. […] ProofBox représente une réponse "concrète" aux défis posés par l'augmentation constante des données numériques dans les enquêtes criminelles." READ MORE

Source: Eurojust

Date: 12 June 2024

Eurojust supports authorities in dismantling EUR 113 million fraudulent investment scheme

"A fraudulent pyramid scheme was taken down by authorities from Germany, Switzerland, Austria, Czechia, Lithuania and Liechtenstein, with the support of Eurojust and Europol. The organised crime group (OCG) used an investment model that focused on the leasing and subleasing of cryptocurrency machines, such as exchange machines and hardware for mining. The suspects were able to target thousands of victims, causing losses of up to EUR 113 million. During an action day on 11 June, six arrests were made, 29 searches were conducted and the suspects' assets were frozen." READ MORE

Source: X, Sport & Citoyenneté

Date: 04 June 2024

85 % des athlètes affirment être confrontés à des actes de cyberviolence (Comité National Olympique et Sportif Français)

"A l'approche des Jeux Olympiques et Paralympiques, les témoignages d'athlètes victimes de cyber-harcèlement s'enchaînent. Face à ce déferlement, cette année comme toutes les autres, Sport & Citoyenneté affirme son engagement contre la haine en ligne." READ MORE

RELATED ARTICLE:

World Economic Forum, Paris Olympics 2024: Cybersecurity experts sound the alarm on cyber threats, 13 June 2024

Source: Trust Pair

Date: 10 June 2024

Deep fake à 25 millions : la fraude aurait-elle pu être évitée ?

"Février 2024 : Arup, multinationale britannique victime de fraude via l'utilisation du deep fake perd 25 millions de dollars. […] L'entreprise basée à Hong Kong a été la cible d'une arnaque d'un genre inédit, mettant en scène des deepfakes vocaux et vidéos d'employés. Un salarié a été piégé lors d'une visioconférence fictive, réunissant apparemment plusieurs de ses collègues. Méfiant au départ, il a fini par être convaincu par la mise en scène réaliste des deep fakes pré-enregistrés." READ MORE

Source: Cyber Security Intelligence

Date: 07 June 2024

Fake News & Disinformation In Poland

"The Polish government has said that a recent false story stating that citizens would be mobilised to fight in Ukraine that appeared on the PAP national news agency was likely a Russian cyber attack. Prime Minister Donald Tusk described the hacking attack as part of Russia's attempts to destabilise the European Parliament elections. The fake news report is probably the work of Russia-sponsored hackers and was designed to interfere with the upcoming European Parliament election, according to Polish sources." READ MORE

RELATED ARTICLE:

NPR, This is what Russian propaganda looks like in 2024, 06 June 2024

Source: Council of Europe

Date: 12 June 2024

Advanced Training for Police and Prosecution on Investigation and Seizure of Cryptocurrencies

"From 12 to 14 June, the European Union-Council of Europe joint project CyberSEE, in close cooperation with OSCE Mission to Serbia and the Serbian Ministry of Interior, Service for Combating High-Tech Crime, organised the Advanced Training for Police and Prosecution on Investigation and Seizure of Cryptocurrencies. Tailored for Serbian cybercrime investigators, prosecutors and digital forensics experts, the training addressed the suspect cryptocurrencies transactions from both investigative and confiscation perspectives. The activity is the first of a planned series of three advanced courses for 2024, designed to enhance the practical skills of the criminal justice practitioners on virtual currencies."

Source: BleepingComputer

Date: 14 June 2024

Keytronic confirms data breach after ransomware gang leaks stolen files

"PCBA manufacturing giant Keytronic is warning it suffered a data breach after the Black Basta ransomware gang leaked 530GB of the company's stolen data two weeks ago. Key Tronic, better known as Keytronic, is an American technology company that initially started as an Original Equipment Manufacturer (OEM) of keyboards and mice but is now one of the largest manufacturers of printed circuit board assembly (PCBA)." READ MORE

Source: BleepingComputer

Date: 14 June 2024

London hospitals cancel over 800 operations after ransomware attack

"NHS England revealed today that multiple London hospitals impacted by last week's Synnovis ransomware attack were forced to cancel hundreds of planned operations and appointments. Formerly known as Viapath, Synnovis was established as GSTS Pathology in 2009 and switched to the Synnovis brand in October 2022. The organization was established as a partnership between SYNLAB UK & Ireland, Guy's and St Thomas' NHS Foundation Trust, and the King's College Hospital NHS Foundation Trust." READ MORE

Source: BleepingComputer

Date: 4 June 2024

Major London hospitals disrupted by Synnovis ransomware attack

"A ransomware attack affecting pathology and diagnostic services provider Synnovis has impacted healthcare services at multiple major NHS hospitals in London. While Synnovis has yet to issue a public statement regarding the June 3 ransomware attack, memos sent by partner hospitals affected by the attack revealed that this "ongoing critical incident" has had a "major impact" on healthcare services across southeast London." READ MORE

RELATED ARTICLES:

The Independent, Qilin: What we know about the Russian gang behind London hospital cyber attack, 05 June 2024

Cybernews, Ransomware attack chaos at London hospitals blamed on Qilin gang, 06 June 2024

Source: CRN

Date: 14 June 2024

CISA Confirms Windows Privilege Escalation Flaw Has Seen Exploitation

"The U.S. Cybersecurity and Infrastructure Security Agency (CISA) confirmed that a Microsoft Windows privilege escalation vulnerability has seen exploitation in attacks. The vulnerability (tracked at CVE-2024-26169) this week was tied to attacks by the Black Basta ransomware gang by researchers at Symantec. The Windows Error Reporting Service Improper Privilege Management Vulnerability was disclosed and fixed by Microsoft in mid-March." READ MORE

RELATED ARTICLES:

CRN, Black Basta Ransomware Attack Brought Down Ascension IT Systems: Report, 10 May 2024

Bleeping Computer, CISA warns of Windows bug exploited in ransomware attacks, 14 June 2024

heise.de, CISA warns: Critical PHP bug is being exploited by ransomware, 14 June 2024

Source: BleepingComputer

Date: 14 June 2024

Panera Bread likely paid a ransom in March ransomware attack

"Panera Bread, an American chain of fast food restaurants, most likely paid a ransom after being hit by a ransomware attack, suggests language used an internal email sent to employees. Last week, Panera began sending data breach notifications to employees, warning that threat actors stole personal information in a March cyberattack that included names and social security numbers. While Panera has not publicly disclosed details about their attack, BleepingComputer first reported that Panera Bread suffered a ransomware attack that encrypted all of its virtual machines." READ MORE

Source: BleepingComputer

Date: 11 June 2024

TellYouThePass ransomware exploits recent PHP RCE flaw to breach servers

"The TellYouThePass ransomware gang has been exploiting the recently patched CVE-2024-4577 remote code execution vulnerability in PHP to deliver webshells and execute the encryptor payload on target systems. Attacks started on June 8, less than 48 hours after the release of security updates by PHP's maintainers, and relied on publicly available exploit code. TellYouThePass ransomware is known for quickly jumping on public exploits for vulnerabilities with a wide impact." READ MORE

Source: BleepingComputer

Date: 06 June 2024

New Fog ransomware targets US education sector via breached VPNs

"A new ransomware operation named 'Fog' launched in early May 2024, is using compromised VPN credentials to breach the networks of educational organizations in the U.S. Fog was discovered by Artic Wolf Labs, which reported that the ransomware operation has not set up an extortion portal yet and was not observed stealing data. However, BleepingComputer can confirm the ransomware gang steals data for double-extortion attacks […]." READ MORE

Source: BleepingComputer

Date: 06 June 2024

Ukraine says hackers abuse SyncThing tool to steal data

"The Computer Emergency Response Team of Ukraine (CERT-UA) reports about a new campaign dubbed "SickSync," launched by the UAC-0020 (Vermin) hacking group in attacks on the Ukrainian defense forces. The threat group is linked to the Luhansk People's Republic (LPR) region, which Russia has occupied almost in its entirety since October 2022. The hacker's activities commonly align with Russia's interests. The attack utilizes the legitimate file-syncing software SyncThing in combination with malware called SPECTR." READ MORE

Source: Euronews

Date: 07 June 2024

Dutch cyberattacks latest in EU election campaign marred by disruption and violence

"Apparent cyberattacks on EU political parties are just the latest round of disruption to an election campaign that has become increasingly fractious. From 6-9 June, hundreds of millions of voters are going to the polls in one of the world's biggest democratic exercises – after a months-long period that has been marked by both peaceful protest and, occasionally, physical violence. Pro-Kremlin hackers have claimed responsibility for a series of attacks on Dutch websites on Thursday (6 June) – the day that voters in the Netherlands went to the polls to select their 31 MEPs for the next five years." READ MORE

RELATED ARTICLES:

Cloudfare.com, Dutch political websites hit by cyber attacks as EU voting starts, 06 June 2024

Bleeping Computer, DDoS attacks target EU political parties as elections begin, 08 June 2024

Latest reports

- Ciberseguridad, El promedio de ciberataques a equipos OT en 2023, fue del 38.6%, 01 June 2024
- AAG, The Latest 2024 Cyber Crime Statistics (updated June 2024), 01 June 2024
- Restore Privacy, Six VPN Apps Introduced Botnet Malware on Systems Since 2014, 01 June 2024
- Samcurry, Hacking Millions of Modems (and Investigating Who Hacked My Modem), 03 June 2024
- VoxAfrica, Aperçus du rapport annuel de référence sur l'hameçonnage de KnowBe4 – Naviguer dans les cybermenaces en Afrique, 03 June 2024
- CheckPoint, Inside the Box: Malware's New Playground, 03 June 2024
- CSIS, Untapping the Full Potential of CLOUD Act Agreements, 06 June 2024
- Statista, Les bots représentent désormais près de 50 % du trafic web, 06 June 2024
- Youth Kiawaaz, "7000 Cyber Crimes Are Being Recorded Daily As Of May 2024": Report Reveals, 07 June 2024
- World Economic Forum, 3 ways manufacturers can build a culture of cyber resilience, 07 June 2024
- Economis, El 78% de las organizaciones en LATAM reconocen que la ciber resiliencia es clave para garantizar la continuidad del negocio, 10 June 2024
- Eurojust, New report on encryption in criminal matters stresses balance between security and privacy, 10 June 2024
- SecureList, Bypassing 2FA with phishing and OTP bots, 10 June 2024
- Skim AI, 5 Deepfake Stats You Need to Know for 2024, 10 June 2024
- GC Mais, PMEs no Brasil sofrem 192 milhões de tentativas de ataques cibernéticos por ano, 10 June 2024
- Global Initiative Alliance, Monitoring online illegal wildlife trade, 10 June 2024
- Nature, Cortical-striatal brain network distinguishes deepfake from real speaker identity, 11 June 2024
- Zscaler, A Brief History of SmokeLoader, Part 1, 11 June 2024
- Europol, First Report on Encryption, 11 June 2024
- Google Cloud, Insights on Cyber Threats Targeting Users and Enterprises in Brazil, 12 June 2024
- Elastic Security Labs, Dipping into Danger: The WARMCOOKIE backdoor, 12 June 2024
- Techopedia, 50 Estadísticas Clave de Ciberseguridad para Junio de 2024, 13 June 2024
- DarkReading, How Cybercrime Empires Are Built, 13 June 2024
- World Bank Group, World Bank Group Gender Strategy 2024 – 2030, 13 June 2024
- World Economic Forum, The brain computer interface market is growing – but what are the risks?, 14 June 2024
- Aethelios, [EN] Unsecure time-based secret and Sandwich Attack - Analysis of my research and release of the "Reset Tolkien" tool, 14 June 2024
- Pulse, Cybermenaces en Afrique : INTERPOL a procédé à 10490 arrestations, 15 June 2024

Upcoming events

- 11-20 June 2024, C-PROC/ BELGIUM/ THE NETHERLANDS, (in person), Study visit to Europe of a delegation of judges from Thailand, GLACY-e
- 17 June 2024, C-PROC/FRANCE, (hybrid), 1st Steering Committee of the GLACY-e project, GLACY-e
- 17 June 2024, C-PROC/FRANCE, (in person), CyberSEE Project Launch and 1st Steering Committee Meeting, Strasbourg, CyberSEE
- 17 June 2024, C-PROC/FRANCE, in person, Regional meeting for criminal justice authorities to agree on regional priorities for criminal justice action on cybercrime and e-evidence and OCSEA, Strasbourg, CyberSEE
- 17-19 June 2024, C-PROC/LITHUANIA, (in-presence), EuroDIG 2024 - Workshop on Cyber Resilience, CyberEast+
- 17-20 June 2024, C-PROC/FRANCE, (in-presence), Project Planning Meeting, CyberEast+
- 17 June 2024, C-PROC/T-CY/ FRANCE, (in person), Bureau Meeting, T-CY
- 18-20 June 2024, C-PROC/T-CY/FRANCE, (hybrid), 30th T-CY Plenary, T-CY
- 19-20 June 2024, C-PROC/ITALY, (online), contribution to the Cybersecurity days organized by the Italian Bar Council in the framework of the EU/CoE Project "Rule of Law and Fundamental Rights - HELP", CyberSouth+
- 20 – 21 June 2024, C-PROC/FRANCE, (in person), Launching event, CyberSPEX
- 24 – 27 June 2024, C-PROC/T-CY/THAILAND, (in person), Introductory Judicial Training on cybercrime and e-evidence in Thailand, T-CY, Octopus
- 24 - 27 June 2024, C-PROC/MAURITIUS, (in person), E-evidence training first responders course (national pilot course, FR language), GLACY-e
- 25 June 2024, T-CY/FRANCE, (in person), Regional workshop Presentation of findings from national gap analyses of the legal and policy framework to combat OCSEA and co-operation with international mechanisms, T-CY
- 25 June 2024, C-PROC/ALBANIA, (in person), Regional meeting of LEAs and CERTs on emerging cyber threats and timely exchange of cyber threat information (with AL EMPACT OAP 8.2), Tirana, CyberSEE
- 25-26 June 2024, C-PROC/EGYPT, (in person), Visit to Egypt to discuss with all relevant national authorities co-operation under the CyberSouth+ project, CyberSouth+
- 26 – 28 June 2024, C-PROC/T-CY/MALAYSIA, (in person), Workshop on legislation, capacities and interagency cooperation in Malaysia, T-CY, Octopus
- 28 June 2024, C-PROC/FRANCE, (online), Meeting with INTERPOL to discuss co-operation and activities with Tunisia, CyberSouth+

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