Cyber News July 2024

On behalf of the Yuval Ne'eman Workshop for Science, Technology and Security, we are happy to share some of the most interesting events and developments that took place in July 2024

July 1 – Australia Unveiled New Plan to Enhance Health Sector Cybersecurity – Australia's Department of Home Affairs will allocate 6.4 million Australian Dollars (AUD) (approximately 4.31 million USD) to establish an Information Sharing and Analysis Center (ISAC), supporting the Australian health sector in combating cybercrime. The ISAC aims to foster cooperation and share information and strategies to mitigate cyber threats among government entities, private and non-profit organizations, and the country's health systems.

July 2 – Japan Revealed New Strategy for Strengthening its Military Cyber Forces – The strategy's primary objective is to recruit 4,000 new cybersecurity experts for Japan's Self-Defense Forces (SDF) between the fiscal years 2025 and 2027. To achieve this goal, the Defense Ministry plans to introduce a specialized test category to identify potential candidates before they are drafted. Furthermore, the ministry will facilitate the exchange of skilled personnel between the SDF and the private sector. Additionally, the Japan Ground Self-Defense Force (JGSDF) High Technical School aims to double the enrollment in its cybersecurity course from 30 to 60 students starting in the fiscal year of 2025.

July 2 – Singapore Launched a Global Competition for Developing Secure Large Language Models – The Cyber Security Agency (CSA) of Singapore, through its CyberSG R&D Programme Office (CRPO) and in collaboration with AI Singapore, has initiated the Global Challenge for Safe and Secure LLMs. Running until October 16, 2024, the competition seeks to develop techniques to safeguard LLMs from jailbreaking attacks. It features two distinct tracks: an attack track, where participants will devise automated methods to induce 75 types of undesirable behaviors in the models, such as disseminating false information, and a defense track, where participants will create protective measures to defend against sophisticated jailbreaking attacks demonstrated in the attack track.

July 9 – American Tech Firms Published New Insights into Houthi Cyber Attacks in the Middle East – The American cybersecurity company LookOut published a blog post revealing that an unnamed hacker group has been conducting cyber espionage attacks against approximately 450 military personnel in Saudi Arabia, Egypt, and other Middle Eastern countries since October 2019. The hackers implanted a GuardZoo spyware on the victims' phones, enabling them to steal photos and documents and track their locations. Additionally, a report by Recorded Future disclosed that the pro-Houthi hacker group OilAlpha stole login credentials from international humanitarian organization workers in Yemen by distributing malicious applications disguised as the organizations' websites. This credential theft allowed OilAlpha operatives to sell access and gather information on the distribution of humanitarian assistance, intending to seize control over it.

July 10 – NATO to Establish Advanced Cyber Defense Center in Belgium – During the annual NATO conference in Washington, D.C., Alliance members announced their plans to establish a new Cyber Defense Center (NICC) at the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium. The center aims to enhance the Alliance's ability to defend against sophisticated cyber threats and bolster overall cybersecurity resilience. It will bring together civilian and military experts across the Alliance, leveraging advanced technology to improve situational awareness and collective cyber defense. The center will also provide military commanders with critical information on cyber threats and vulnerabilities, including those affecting privately owned critical infrastructures integral to the Alliance's military operations.

Make sure you don't miss the latest on cyber research

Join our mailing list