Cyber News August 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 August 2024

August 6 – Ireland Published National Cyber Emergency Plan to Enhance National Cybersecurity – Ireland's National Cyber Security Center (NCSC-IR) released the National Cyber Emergency Plan (NCEP) to address cyber incidents that could impact critical IT and OT systems and networks. The plan outlines three operational modes to enhance national cybersecurity. In "Permanent Mode", the NCSC and the government work to maintain situational awareness by gathering reports on potential security threats and vulnerabilities from the public sector and other entities. "Warning Mode" is activated when there are signs of a potential cyber emergency, either within Ireland or abroad. At this point, the NCSC guides affected entities on preparedness and response. "Full Activation Mode" is employed amid an active cyber emergency, during which the NCSC oversees all necessary government actions to contain, mitigate, and recover from the incident.

August 7 – Singapore Formed Task Force to Boost Digital Resilience Following CrowdStrike Outage – In response to CrowdStrike's interruption on July 19, 2024, Singapore's Minister of Digital Development and Information (MDDI), Josephine Teo, has formed a task force to enhance the nation's digital resilience. The task force will undertake comprehensive assessments of the country's IT systems and protocols and collaborate with both public and private sectors to formulate robust strategic plans to prevent similar incidents.

August 9 – UK Intends to Launch a New Lab for Tackling AI-based Cyber Threats – The United Kingdom's Prime Minister Office, Keir Starmer, in conjunction with GCHQ, plans to set up a specialized laboratory dedicated to researching AI-driven threats, including cyber-attacks, disinformation, and the potential use of biological weapons. This facility will bring together representatives from government and intelligence agencies, technology firms, academic experts, and international partners. The creation of this laboratory is a strategic effort by Britain to address and counteract cyber threats and misinformation emanating from state actors, particularly Russia and China.

August 9 – Microsoft Revealed Foreign Influence Campaigns Targeting the 2024 United States Presidential Elections – The Microsoft Threat Analysis Center (MTAC) has released a report detailing cyber-attacks and influence operations conducted by US adversaries aimed at disrupting local politics and the upcoming presidential elections in November 2024. The report identifies the Storm-2035 network, comprised of four websites that disseminate misleading and inflammatory content on various topics, including the presidential race and the Israel-Hamas conflict. This network, managed by an unidentified Iranian entity, employed Artificial intelligence to replicate and spread content from other sources. Concurrently, US intelligence agencies, including the FBI, have confirmed that Iranian hackers targeted Donald Trump's campaign to meddle in the election. Additionally, the Storm-1852 group, linked to the Chinese government, has been circulating short videos on social media, criticizing President Joe Biden's administration and questioning his fitness for office. Meanwhile, the Storm-1516 group, associated with Russia, has been disseminating false information since April 2024 to undermine US-Ukraine relations. This includes claims that the CIA director directed a Ukrainian troll farm to influence the election process and skew its outcomes.

Overall, there is a noticeable divergence in these nations' influence strategies. Russia focuses on deepening domestic divisions and eroding trust in the US government to disrupt the election process. In contrast, Iran aims to prevent Trump's re-election. Therefore, Iran has intensified its activities to influence election outcomes by focusing on particular demographic groups, including swing state voters. Meanwhile, Russia is leveraging AI to create fake profiles and spread favorable messages. At the same time, China primarily uses AI to produce and disseminate politically charged images and videos to exacerbate US political disputes.

August 12 – Japan to Establish a New Research Institute for Enhancing Cyberwarfare Research - Japan's Ministry of Defense has revealed plans to inaugurate a new research center, the Defense Innovation Technology Institute (DITI), in October 2024. This center will focus on advancing technologies for military applications, cyber warfare, and artificial intelligence, drawing on research methodologies similar to those used by the US Department of Defense's Innovation Unit (DIU) and Defense Advanced Research Projects Agency (DARPA). Operating under the Acquisition, Technology & Logistics Agency (ATLA), the institute will employ approximately 100 researchers, with half sourced from the private sector and academia. Additionally, it will function as a research institute that tracks global advancements in technology and manages projects involving dual-use technologies. This initiative is part of Japan's national defense strategy outlined in December 2022, aimed at fostering innovation in defense capabilities.

Make sure you don't miss the latest on cyber research
Join our mailing list