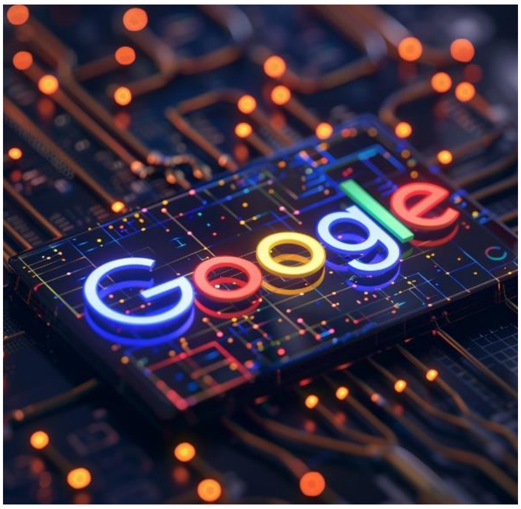
Cybersecurity Pulse

Updated 19th Feb 2024

Dive into this week's essential roundup of cybersecurity news for the telecoms industry. From groundbreaking technologies to pivotal regulatory updates, we bring you the latest news and analyses to keep you informed and one step ahead.

Google launches a slew of AI initiatives to enhance cybersecurity



Google has launched a series of AI initiatives to bolster cybersecurity, including the AI Cyber Defence Initiative and the open-sourcing of Magika, an AI-powered tool for identifying malware. The company aims to use AI to address the "Defender's Dilemma" and enhance the transatlantic cybersecurity ecosystem through internationalisation strategies and skill development.

As part of this effort, Google has announced $2 million in research grants and strategic partnerships with several institutes, as well as the expansion of its $15 million Google.org Cybersecurity Seminars Program to cover Europe. The AI Cyber Defence Initiative is built on Google's Secure AI Framework (SAIF), introduced last year to mitigate the risks associated with AI systems.

These initiatives demonstrate Google's commitment to leveraging AI for cybersecurity and fostering collaboration with the developer community and academic institutions to advance cyber defence capabilities.

Source: CSO Online

Russian-Linked Hackers Target 80+ Organizations via Roundcube Flaws

Russian-linked hackers have targeted over 80 organisations, primarily in Georgia, Poland, and Ukraine, in a new cyber espionage campaign. The threat actor, known as Winter Vivern or TA473, exploited cross-site scripting (XSS) vulnerabilities in Roundcube webmail servers to gain unauthorized access to targeted mail servers, aiming to collect intelligence on European political and military activities. The attack involved the exploitation of Roundcube flaws to deliver JavaScript payloads designed to exfiltrate user credentials to a command-and-control (C2) server.

The campaign, attributed to Threat Activity Group 70 (TAG-70), demonstrated a high level of sophistication in its attack methods, leveraging social engineering techniques and exploiting security vulnerabilities to bypass the defences of government and military organizations.

Source: Hacker News

Australia's Eagers Automotive warns of potential data leak

Australia's Eagers Automotive has issued a warning about a potential data leak after a third party claimed to have published data allegedly obtained from the company's servers. The automotive retailer is investigating the claim and assessing the nature of the compromised data, while also reaching out to affected individuals and monitoring for any further data publication claims. The company experienced a cyber incident in December, which led to outages across its operations in Australia and New Zealand, affecting its ability to finalize transactions for several vehicles.

An investigation revealed that a third party had hacked into the company's servers, gaining unauthorized access to parts of its IT systems. Despite the initial operational impact, the company stated that it does not anticipate a 'material' financial impact from the event for fiscal 2024. Eagers Automotive did not immediately provide details on the type of data that was purportedly leaked

Source: Reuters

Mysterious ‘MMS Fingerprint’ Hack Used by Spyware Firm NSO Group Revealed

The spyware firm NSO Group has been revealed to have developed a new potential infection technique termed "MMS Fingerprint," which can silently extract device information during MMS retrieval, without user interaction. This method, hinted at in a contract between NSO and Ghana’s telecom regulator, is designed to reveal target device and operating system information, and could streamline further attacks by tailoring payloads or crafting phishing campaigns based on device specifics.

While there is no indication that this technique is currently being used, its existence and NSO’s indication of availability raise concerns about potential exploitation. The method is said to be applicable to Android, Blackberry, and iOS, and can be blocked and potentially mitigated by users disabling MMS auto-retrieval.

Source: Security Week

As we wrap up this week’s cybersecurity journey, remember that staying informed is the key to resilience in our fast-paced industry. We hope the insights shared have empowered you with knowledge and sparked ideas for safeguarding our digital frontiers. Let’s continue to build a secure, connected world together. Until next time, keep your networks safe and your data secure.

Cybersecurity Pulse