23 June 25

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

Russian Hackers Bypass Gmail MFA With App-Specific Password Ruse

A professional hacking team linked to the Russian government has been caught wielding a new, low-and-slow phishing trick that beats two-factor authentication by exploiting Google's little-known "app-specific password" feature. According to documentation from Google's Threat Intelligence Group, the operation ran from April into early June and impersonated US State Department officials in email threads with flawless English and copied to four bogus @state.gov colleagues. Google tracks the threat actor as UNC6293 and believes it is linked to APT29, the Russian intelligence unit blamed for the 2016 Democratic National Committee breach. Investigators estimate the group spent weeks cultivating each target before pushing detailed instructions on the ASP (application-specific password) feature.

https://www.securityweek.com/russian-hackers-bypass-gmail-mfa-with-app-specific-password-ruse/

Healthcare Services Company Episource Data Breach Impacts 5.4 Million People

Episource is a U.S.-based healthcare services and technology company that provides risk adjustment services, clinical data analytics, and medical record review solutions to health plans and healthcare organizations, particularly those operating in Medicare Advantage, Medicaid, and ACA markets. On February 6, 2025, the company detected suspicious activity in its systems. A threat actor accessed and copied data between January 27 and February 6. In response to the security breach, Episource shut down its systems, launched an investigation with the help of experts, and notified law enforcement. The firm is not aware of any reported misuse of the data so far. The exposed data varied by individual and may have included contact details, health insurance info, medical records, and, in limited cases, Social Security numbers or birth dates. Though financial data was mostly unaffected, individuals should monitor health, financial, and tax records for suspicious activity and report any anomalies to relevant institutions or authorities.

https://securityaffairs.com/179115/data-breach/healthcare-services-company-episource-data-breach-impacts-5-4-million-people.html

China-Linked Group Salt Typhoon Breached Satellite Firm Viasat

China-linked APT group Salt Typhoon hacked the satellite communications firm Viasat, the cyber-espionage group has previously breached the networks of multiple other telecom providers in the United States and globally. Viasat is a global communications company based in Carlsbad, California, that specializes in satellite-based connectivity solutions across multiple sectors. The intrusion was discovered earlier this year and the company investigated the security breach with the help of federal authorities. Viasat said it investigated unauthorized access with a cybersecurity partner and found no evidence that customers were affected. China-linked APT group Salt Typhoon (also known as FamousSparrow and GhostEmperor) and has been active since at least 2019 and targeted government entities and telecom companies.

https://securityaffairs.com/179146/security/china-linked-group-salt-typhoon-breached-satellite-firm-viasat.html

New Android Malware Surge Hits Devices via Overlays, Virtualization Fraud, and NFC Theft

Cybersecurity researchers exposed the inner workings of an Android malware called AntiDot that has compromised over 3,775 devices as part of 273 unique campaigns. AntiDot is advertised as a "three-in-one" solution with

capabilities to record the device screen by abusing Android's accessibility services, intercept SMS messages, and extract sensitive data from third-party applications. The Android botnet is suspected to be delivered via malicious advertising networks or through highly tailored phishing campaigns based on activity that indicates selective targeting of victims based on language and geographic location. AntiDot was first publicly documented in May 2024 after it was spotted being distributed as Google Play updates to accomplish its information theft objectives. Like other Android trojans, it features a wide range of capabilities to conduct overlay attacks, log keystrokes, and remotely control infected devices using Android's MediaProjection API. It also establishes a WebSocket communication to facilitate real-time, bi-directional communication between the infected device and an external server.

https://thehackernews.com/2025/06/new-android-malware-surge-hits-devices.html

Steelmaker Nucor Says Hackers Stole Data in Recent Attack

American steel giant Nucor Corporation shared an update on the recent cyberattack, confirming that hackers have taken some data from its systems. Nucor, which claims to be the largest steel manufacturer and recycler in North America, disclosed the cybersecurity incident in mid-May. The attack involved unauthorized access to IT systems and resulted in some systems being taken offline and the temporary halting of certain production operations. Nucor on Friday shared an update on the incident in a filing with the Securities and Exchange Commission (SEC). The company's investigation showed that the threat actor managed to exfiltrate "limited data" from the compromised IT systems. Systems taken offline in response to the cyberattack have been restored and the company told the SEC that the incident is unlikely to have a material impact on its financial condition or results of operations. Nucor believes the threat actor has been locked out of its systems and it has taken steps to prevent future breaches.

https://www.securityweek.com/steelmaker-nucor-says-hackers-stole-data-in-recent-attack/

WordPress Motors Theme Flaw Mass-Exploited to Hijack Admin Accounts

Hackers are exploiting a critical privilege escalation vulnerability in the WordPress theme "Motors" to hijack administrator accounts and gain complete control of a targeted site. The malicious activity was spotted by Wordfence, which had warned last month about the severity of the flaw, tracked under CVE-2025-4322, urging users to upgrade immediately. Motors, developed by StylemixThemes, is a WordPress theme popular among automotive-related websites. It has 22,460 sales on the EnvatoMarket and is backed by an active community of users. The privilege escalation vulnerability was discovered on May 2, 2025, and first reported by Wordfence on May 19, impacting all versions before and including 5.6.67. The flaw arises from an improper user identity validation during password updating, allowing unauthenticated attackers to change administrator passwords at will.

https://www.bleepingcomputer.com/news/security/wordpress-motors-theme-flaw-mass-exploited-to-hijack-admin-accounts/

743,000 Impacted by McLaren Health Care Data Breach

Michigan healthcare provider McLaren Health Care is notifying over 743,000 people that their personal information was compromised in a 2024 data breach. The incident, the organization says, was discovered on August 5, 2024, after suspicious activity was identified on computer systems pertaining to McLaren and Karmanos Cancer Institute. In a written notification to the impacted individuals, a copy of which was submitted to the Maine Attorney General's Office, McLaren revealed that ransomware was involved in the attack. The hackers had access to its network between July 17 and August 3, and obtained various files containing sensitive data, including personally identifiable information (PII) and protected health information (PHI). The potentially compromised information, the organization says, includes names, Social Security numbers, driver's license numbers, health insurance details, and medical

information. McLaren notified the Maine AGO that 743,131 individuals were impacted by the data breach and that it is providing them with 12 months of free credit monitoring services, as well as with guidance on how to protect themselves against fraud and identity theft.

https://www.securityweek.com/743000-impacted-by-mclaren-health-care-data-breach/

US Braces for Cyberattacks After Bombing Iranian Nuclear Sites

Iranian threat actors are expected to intensify their cyberattacks against the United States following President Donald Trump's decision to launch air strikes on Iran. After the US bombed three key nuclear sites in Iran, the regime in Tehran vowed to retaliate. The Department of Homeland Security (DHS) issued a national terrorism advisory system bulletin on Sunday, warning that the Iranian government has publicly condemned the United States' involvement in the conflict and that retaliation could come in several forms. Iran could conduct lethal attacks and commit acts of violence on US soil, but Iranian state-sponsored hackers and pro-Iran hacktivists are also likely to intensify attacks against the United States in response to recent events. The cybersecurity community has closely followed Iran's activities in cyberspace. While some attacks linked to Iranian hackers appeared unsophisticated — including attacks targeting industrial control systems (ICS) — others were more advanced. This includes phishing attacks aimed at political campaigns, and brute force attacks targeting critical infrastructure. In terms of malware, the community has seen noteworthy threats designed for intelligence gathering, as well as malware delivery methods.

https://www.securityweek.com/us-braces-for-cyberattacks-after-joining-israel-iran-war/