9 June 25

Cyber Threat Roundup

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

Contents

Articles 2
Trump Cybersecurity Executive Order Targets Digital Identity, Sanctions Policies 2
Microsoft Helps CBI Dismantle Indian Call Centers Behind Japanese Tech Support Scam 2
North Face and Cartier Customer Data Stolen in Cyber Attacks 2
ConnectWise Hit by Cyberattack; Nation-State Actor Suspected in Targeted Breach 2
New Linux Flaws Allow Password Hash Theft via Core Dumps in Ubuntu, RHEL, Fedora 3
UNC1151 Exploiting Roundcube to Steal User Credentials in a Spearphishing Campaign 3
Department Files Civil Forfeiture Complaint Against Over $7.74M Laundered on Behalf of the North Korean Government 3

Articles

Trump Cybersecurity Executive Order Targets Digital Identity, Sanctions Policies

According to a fact sheet published by the White House, the new order aims to improve software development, border gateway (BGP) security, post-quantum cryptography implementation, AI security, IoT security, the use of encryption, and sanctions policies, as well as to prevent the abuse of digital identities. Specifically, the new executive order (EO) targets EO 14144, which Biden signed in January 2025, just before Trump took office. The order signed by Trump last week strikes out and replaces several subsections of EO 14144. One section that was completely removed covered the use of digital identities, encouraging the acceptance of digital identity documents to access public benefits programs that require identity verification.

https://www.securityweek.com/trump-cybersecurity-executive-order-targets-digital-identity-sanctions-policies/

Microsoft Helps CBI Dismantle Indian Call Centers Behind Japanese Tech Support Scam

India's Central Bureau of Investigation (CBI) has revealed that it has arrested six individuals and dismantled two illegal call centers that were found to be engaging in a sophisticated transnational tech support scam targeting Japanese citizens. The law enforcement agency said it conducted coordinated searches at 19 locations across Delhi, Haryana, and Uttar Pradesh on May 28, 2025, as part of an initiative called Operation Chakra V, which aims to combat cyber-enabled financial crimes. The cybercrime syndicates, per the CBI, defrauded foreign nationals, mainly Japanese citizens, by masquerading as technical support personnel from various multinational corporations, including Microsoft.

https://thehackernews.com/2025/06/microsoft-helps-cbi-dismantle-indian.html

North Face and Cartier Customer Data Stolen in Cyber Attacks

Fashion brand The North Face and luxury jeweller Cartier have become the latest retailers to report having customer data stolen in cyber attacks. North Face has emailed some customers saying it discovered a "small-scale" attack in April this year. Cartier said "an unauthorized party gained temporary access to our system".

Both brands say data such as customers names and email addresses were taken, but financial information was not. There has been a wave of cyber attacks on high-profile retailers in recent weeks, including Adidas, Victoria's Secret and Harrods. Marks and Spencer (M&S) and the Co-op had their operations severely disrupted when they were targeted in April.

https://www.bbc.com/news/articles/c39x3jpv8lyo

ConnectWise Hit by Cyberattack; Nation-State Actor Suspected in Targeted Breach

Fake ConnectWise, the developer of remote access and support software ScreenConnect, has disclosed that it was the victim of a cyber attack that it said was likely perpetrated by a nation-state threat actor. "ConnectWise recently learned of suspicious activity within our environment that we believe was tied to a sophisticated nation-state actor, which affected a very small number of ScreenConnect customers," the company said in a brief advisory on May 28, 2025. The company said it has engaged the services of Google Mandiant to conduct a forensic probe into the incident and that it has notified all affected customers. The incident was first reported by CRN.

https://thehackernews.com/2025/05/connectwise-hit-by-cyberattack-nation.html

New Linux Flaws Allow Password Hash Theft via Core Dumps in Ubuntu, RHEL, Fedora

Two information disclosure flaws have been identified in apport and systemd-coredump, the core dump handlers in Ubuntu, Red Hat Enterprise Linux, and Fedora, according to the Qualys Threat Research Unit (TRU). Tracked as CVE-2025-5054 and CVE-2025-4598, both vulnerabilities are race condition bugs that could enable a local attacker to obtain access to access sensitive information. Tools like Apport and systemd-coredump are designed to handle crash reporting and core dumps in Linux systems. "These race conditions allow a local attacker to exploit a SUID program and gain read access to the resulting core dump," Saeed Abbasi, manager of product at Qualys TRU, said.

https://thehackernews.com/2025/05/new-linux-flaws-allow-password-hash.html

UNC1151 Exploiting Roundcube to Steal User Credentials in a Spearphishing Campaign

CERT Polska has observed a spear phishing campaign targeting Polish entities this week. The threat actor attempted to exploit the CVE-2024-42009 vulnerability, which allows JavaScript code to be executed when an email message is opened, with the aim of stealing user credentials. It's also worth noting that a new vulnerability in Roundcube, CVE-2025-49113, was discovered just this week. It allows an authenticated attacker to execute code and potentially take over the entire webmail server. While we haven't observed any signs of this vulnerability being exploited, it could be combined with an account compromise vulnerability to form a highly effective attack chain. Based on technical indicators, we attribute this campaign to a cluster of UNC1151 activity with high confidence. According to publications by Mandiant and Google, UNC1151 is associated with the Belarusian government while other sources connect it with Russian intelligence services.

https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

Department Files Civil Forfeiture Complaint Against Over $7.74M Laundered on Behalf of the North Korean Government

The Department of Justice filed a civil forfeiture complaint today in the U.S. District Court for the District of Columbia alleging that North Korean information technology (IT) workers obtained illegal employment and amassed millions in cryptocurrency for the benefit of the North Korean government, all as a means of evading U.S. sanctions placed on North Korea. The funds were initially restrained in connection with an April 2023 indictment against Sim Hyon Sop (Sim), a North Korean Foreign Trade Bank (FTB) representative who was allegedly conspiring with the IT workers. While the North Koreans were attempting to launder those ill-gotten gains, the U.S. government was able to freeze and seize over $7.74 million tied to the scheme. “This forfeiture action highlights, once again, the North Korean government’s exploitation of the cryptocurrency ecosystem to fund its illicit priorities,” said Matthew R. Galeotti, Head of the Justice Department’s Criminal Division. “The Department will use every legal tool at its disposal to safeguard the cryptocurrency ecosystem and deny North Korea its ill-gotten gains in violation of U.S. sanctions.”

https://www.justice.gov/opa/pr/department-files-civil-forfeiture-complaint-against-over-774m-laundered-behalf-north-korean