



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

11 Feb 25

Cyber Threat Roundup

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

Contents

Articles	2
Operation Phobos Aetor: Police Dismantled 8Base Ransomware Gang	2
Apple Fixes Zero-Day Flaw Exploited in “Extremely Sophisticated” Attack (CVE-2025-24200)	2
Hacker Pleads Guilty to SIM Swap Attack on US SEC X Account.....	2
Hackers Exploit Google Tag Manager to Deploy Credit Card Skimmers on Magento Stores	3
Cyberattack Disrupts Lee Newspapers' Operations Across the US.....	3

Articles

Operation Phobos Aetor: Police Dismantled 8Base Ransomware Gang

Authorities dismantled the 8Base ransomware gang, shutting down its dark web data leak and negotiation sites. An international law enforcement operation, codenamed Operation Phobos Aetor, dismantled the 8Base ransomware gang. The police took down the dark web data leak and negotiation sites. The police has yet to disclose the names of the suspects. Authorities replaced the seized websites with a law enforcement banner displaying the message: "This hidden site and the criminal content have been seized by the Bavarian State Criminal Police Office on behalf of the Office of the Public Prosecutor General in Bamberg." The police arrested four European citizens in Phuket, Thailand, who are suspected to have stolen over \$16 million through ransomware attacks affecting over 1,000 victims worldwide. The suspects were also accused of stealing approximately 16 million US dollars' worth of Bitcoins from around 1,000 victims worldwide."

<https://securityaffairs.com/174078/cyber-crime/police-dismantled-8base-ransomware-gang.html>

Apple Fixes Zero-Day Flaw Exploited in "Extremely Sophisticated" Attack (CVE-2025-24200)

Users of iPhones and iPads that run iOS/iPadOS 18 and iPadOS 17 are urged to implement the latest updates to plug a security feature bypass vulnerability (CVE-2025-24200) exploited in the wild in "an extremely sophisticated" attack. "A physical attack may disable USB Restricted Mode on a locked device," Apple explained. USB Restricted Mode is a feature Apple introduced in 2018 to protect users against device unlocking ("cracking") tools such as Graykey, usually at the hands of law enforcement. These tools get connected to target devices via USB and can bypass passcode-based protection/encryption to extract data. USB Restricted Mode prevents them from accessing the data through this connection if iPhones and iPads haven't been unlocked for over an hour. "Apple is aware of a report that [CVE-2025-24200] may have been exploited in an extremely sophisticated attack against specific targeted individuals," the company said.

<https://www.helpnetsecurity.com/2025/02/11/apple-fixes-zero-day-flaw-exploited-in-extremely-sophisticated-attack-cve-2025-24200/>

Hacker Pleads Guilty to SIM Swap Attack on US SEC X Account

Today, an Alabama man pleaded guilty to hijacking the U.S. Securities and Exchange Commission (SEC) account on X in a January 2024 SIM swapping attack. This comes after the defendant, 25-year-old Eric Council Jr., first pleaded not guilty to hacking the account and enabling his co-conspirators to make a fake announcement that Bitcoin ETFs were approved. "Today the SEC grants approval to Bitcoin ETFs for listing on registered national security exchanges. The approved Bitcoin ETFs will be subject to ongoing surveillance and compliance measures to ensure continued investor protection," read the fake post on X. Among these searches, investigators found that the defendant was looking for details on "what are the signs that you are under investigation by law enforcement of the FBI even if you have not been contacted by them" and "how can i know for sure if I am being investigate by the FBI." Council is scheduled to be sentenced on May 16 and faces a maximum penalty of five years in prison after pleading guilty to conspiracy to commit aggravated identity theft and access device fraud.

<https://www.bleepingcomputer.com/news/security/hacker-pleads-guilty-to-sim-swap-attack-on-us-sec-x-account/>

Hackers Exploit Google Tag Manager to Deploy Credit Card Skimmers on Magento Stores

Threat actors have been observed leveraging Google Tag Manager (GTM) to deliver credit card skimmer malware targeting Magento-based e-commerce websites. Website security company Sucuri said the code, while appearing to be a typical GTM and Google Analytics script used for website analytics and advertising purposes, contains an obfuscated backdoor capable of providing attackers with persistent access. As of writing, as many as three sites have been found to be infected with the GTM identifier (GTM-MLHK2N68) in question, down from six reported by Sucuri. GTM identifier refers to a container that includes the various tracking codes (e.g., Google Analytics, Facebook Pixel) and rules to be triggered when certain conditions are met. Further analysis has revealed that the malware is being loaded from the Magento database table "cms_block.content," with the GTM tag containing an encoded JavaScript payload that acts as a credit card skimmer. Last week, the U.S. Department of Justice (DoJ) also announced charges against two Romanian nationals, Andrei Fagaras and Tamas Kolozsvari, over their alleged role in a payment card skimming operation. They have been indicted on three counts of access device fraud for possessing skimmers at three different locations in the Eastern District of Louisiana.

<https://thehackernews.com/2025/02/hackers-exploit-google-tag-manager-to.html>

Cyberattack Disrupts Lee Newspapers' Operations Across the US

Lee Enterprises, one of the largest newspaper groups in the United States, says a cyberattack that hit its systems caused an outage last week and impacted its operations. In a Friday filing with the U.S. Securities and Exchange Commission (SEC), the company said the February 3 cyberattack was behind the outage that impacted its business operations. Lee Enterprises newsrooms have reported that the cyberattack forced the company to shut down many of its networks, disrupting the printing and delivery of dozens of newspapers. BleepingComputer has also learned that the resulting outage has caused chaos across the newspaper group, with VPNs used to connect securely to the network not working and reporters and editors unable to access their files. Lee Enterprises was hit by another cyberattack five years ago, before the 2020 U.S. presidential election, when Iranian hackers breached its network as part of a broader campaign to spread disinformation.

<https://www.bleepingcomputer.com/news/security/cyberattack-disrupts-lee-newspapers-operations-across-the-us/>