DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

24 Mar 25

Cyber Threat Roundup

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

Contents

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics DC3 Cyber Crime Center

Articles

New 'Rules File Backdoor' Attack Lets Hackers Inject Malicious Code via AI Code Editors

Cybersecurity researchers disclosed details of a new supply chain attack vector dubbed Rules File Backdoor that affects artificial intelligence (AI)-powered code editors like GitHub Copilot and Cursor, causing them to inject malicious code. The attack vector is notable for the fact that it allows malicious code to silently propagate across projects, posing a supply chain risk. The crux of the attack hinges on the rules files that are used by AI agents to guide their behavior, helping users to define best coding practices and project architecture. Following responsible disclosure in late February and March 2024, both Cursor and GiHub have stated that users are responsible for reviewing and accepting suggestions generated by the tools.

http://thehackernews.com/2025/03/new-rules-file-backdoor-attack-lets.html

Nation-State Actors and Cybercrime Gangs Abuse Malicious .LNK Files for Espionage and Data Theft

At least 11 state-sponsored threat groups have been abusing Windows shortcut files for espionage and data theft, according to an analysis by Trend Micro's Zero Day Initiative (ZDI). Trend ZDI researchers discovered 1,000 malicious .lnk files used by nation-state actors and cybercrime groups to execute hidden malicious commands on a victim's machine by exploiting the vulnerability ZDI-CAN-25373. Since 2017, the vulnerability has been exploited by APT groups from North Korea, Iran, Russia, and China. The attacks carried out by the threat actors aimed at organizations across the government, financial, telecommunications, military, and energy sectors in North America, Europe, Asia, South America, and Australia. Nearly half of the threat actors exploiting ZDI-CAN-25373 are from North Korea (45,5%), with 70% focused on espionage and 20% on financial gain, often interlinked.

https://securityaffairs.com/175569/apt/nation-state-actors-and-cybercrime-gangs-abuse-malicious-lnk-files-for-espionage-and-data-theft.html

New Ad Fraud Campaign Exploits 331 Apps with 60M+ Downloads for Phishing and Intrusive Ads

Cybersecurity researchers warn of a large-scale ad fraud campaign that leveraged hundreds of malicious apps published on the Google Play Store to serve full-screen ads and conduct phishing attacks. Details of the activity were first disclosed by Integral Ad Science (IAS) earlier this month, documenting the discovery of over 180 apps that were engineered to deploy endless and intrusive full-screen interstitial video ads. The ad fraud scheme was codenamed Vapor. These apps, which have since been taken down by Google, masqueraded as legitimate apps and collectively amassed more than 56 million downloads between them, generating over 200 million bid requests daily. It's believed that the campaign is the work of either a single threat actor or several cybercriminals who are making use of the same packing tool that's advertised for sale on underground forums.

https://thehackernews.com/2025/03/new-ad-fraud-campaign-exploits-331-apps.html

ChatGPT SSRF Bug Quickly Becomes a Favorite Attack Vector

Cybersecurity firm Veriti reports that threat actors are exploiting a server-side request forgery (SSRF) vulnerability, tracked as CVE-2024-27564 (CVSS score of 6.5), in ChatGPT to target financial and government organizations in the US. The flaw resides in pictureproxy.php and attackers could exploit the issue to inject URLs via the url parameter to trigger arbitrary requests. The pictureproxy.php file SSRF vulnerability is due to insufficient validation

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

2

of the url parameter. Attackers can exploit this by injecting crafted URLs, leading the server to make arbitrary requests via file_get_contents. Veriti researchers observed over 10K attack attempts in a week from multiple threat actors. Attacks also targeted financial and healthcare firms in Germany, Thailand, Indonesia, Colombia, and the UK.

https://securityaffairs.com/175560/hacking/chatgpt-ssrf-bug-quickly-becomes-a-favorite-attack-vector.html

Kaspersky Links Head Mare to Twelve, Targeting Russian Entities via Shared C2 Servers

Two known threat activity clusters codenamed Head Mare and Twelve have likely joined forces to target Russian entities, new findings from Kaspersky reveal. Both Head Mare and Twelve were previously documented by Kaspersky in September 2024, with the former leveraging a now-patched vulnerability in WinRAR (CVE-2023-38831) to obtain initial access and deliver malware and in some cases, even deploy ransomware families like LockBit for Windows and Babuk for Linux (ESXi) in exchange for a ransom. The activity, the Russian company said, closely resembles another campaign dubbed SHROUDED#SLEEP that Securonix documented in October 2024 as leading to the deployment of a backdoor referred to as VeilShell in intrusions targeting Cambodia and likely other Southeast Asian countries.

https://thehackernews.com/2025/03/kaspersky-links-head-mare-to-twelve.html

Fake Semrush Ads Used to Steal SEO Professionals' Google Accounts

A new phishing campaign is targeting SEO professionals with malicious Semrush Google Ads that aim to steal their Google account credentials. Malwarebytes researcher Jerome Segura and SEO strategist Elie Berreby believe that the threat actor is after Google Ads accounts that would enable them to create new malvertising campaigns. This type of "cascading fraud" has been gaining traction recently, as Malwarebytes uncovered in January a similar operation where fake Google Ads hosted on Google Sites targeted Google Ads accounts. In this latest case, the cybercriminals abuse the Semrush brand, a popular software-as-a-service (SaaS) platform used for SEO, online advertising, content marketing, and competitive research. Semrush is widely used by digital marketers, advertisers, e-commerce businesses, and large enterprises, including 40% of Fortune 500 companies. To avoid getting trapped by Google Ads scams, avoid clicking on promoted/sponsored results, bookmark pages you access frequently to visit them directly, and always double-check that you landed on the official domain before logging in.

https://www.bleepingcomputer.com/news/security/fake-semrush-ads-used-to-steal-seo-professionals-google-accounts/

Microsoft: Exchange Online Bug Mistakenly Quarantines User Emails

Microsoft is investigating an Exchange Online bug causing anti-spam systems to mistakenly quarantine some users' emails. According to a new incident report added to the Microsoft 365 Admin Center, the email issues started almost five hours ago, at 10:11 UTC. While the company has yet to share what regions are impacted, this Exchange Online incident has been tagged as a critical service issue tracked under EX1038119 on the Microsoft 365 admin center. Redmond's engineers are also tracking a separate incident (EX1038200) preventing users and admins from accessing the 'Review' page under the Email and Collaboration section in the Security portal. Customers have been reporting experiencing similar problems over the last two days, including having issues accessing the Quarantine Review page when using Microsoft Defender for 365 for email protection and being unable to release emails from quarantine.

https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-online-bug-mistakenly-quarantines-user-emails/

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics DC3 Cyber Crime Center

3

UAT-5918 Targets Taiwan's Critical Infrastructure Using Web Shells and Open-Source Tools

Threat hunters have uncovered a new threat actor named UAT-5918 that has been attacking critical infrastructure entities in Taiwan since at least 2023. Besides critical infrastructure, some of the other targeted verticals include information technology, telecommunications, academia, and healthcare. Assessed to be an advanced persistent threat (APT) group looking to establish long-term persistent access in victim environments, UAT-5918 is said to share tactical overlaps with several Chinese hacking crews tracked as Volt Typhoon, Flax Typhoon, Tropic Trooper, Earth Estries, and Dalbit. Attack chains orchestrated by the group involve obtaining initial access by exploiting N-day security flaws in unpatched web and application servers exposed to the internet. The foothold is then used to drop several open-source tools to conduct network reconnaissance, system information gathering, and lateral movement.

https://thehackernews.com/2025/03/uat-5918-targets-taiwans-critical.html

Ransomware Group Claims Attack on Virginia Attorney General's Office

An incident became public in mid-February, when the Virginia's top prosecutorial agency told employees that nearly all its computer systems, internal services and applications, and website were down, and that internet connectivity and VPN access were affected as well. Employees were notified of the attack via email and were reportedly directed to return to paper court filings, but the AGO refrained from publicly sharing details on the intrusion. On March 20, however, the Cloak ransomware gang added the Virginia AGO to its Tor-based leak site, making data allegedly stolen from its systems available for download, which suggests that the group failed to extort the AGO. Active since late 2022, Cloak appears to have made over 65 victims to date, but only 13 of its attacks have been confirmed, cybersecurity firm Comparitech notes. The attack on Virginia AGO is its first confirmed attack this year.

https://www.securityweek.com/ransomware-group-claims-attack-on-virginia-attorney-generals-office/

HellCat Hackers Go on a Worldwide Jira Hacking Spree

Swiss global solutions provider Ascom has confirmed a cyberattack on its IT infrastructure as a hacker group known as Hellcat targets Jira servers worldwide using compromised credentials. The company announced in a press release that hackers on Sunday breached its technical ticketing system and is currently investigating the incident. Ascom is a telecommunications company with subsidiaries in 18 countries focusing on wireless on-site communications. HellCat hacking group claimed the attack and told BleepingComputer that they stole about 44GB of data that may impact all of the company's divisions. Ascom says that the hackers compromised its technical ticketing system, the incident had no impact on the company's business operations, and that customers and partners do not need to take any preventive action. HellCat's activity didn't stop at these breaches as the threat actor announced today that they compromised the Jira system of Affinitiv, a marketing company that provides data analytics a platform for OEMs and dealerships in the automotive industry.

https://www.bleepingcomputer.com/news/security/hellcat-hackers-go-on-a-worldwide-jira-hacking-spree/

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

4