



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

21 Feb 25

Cyber Threat Roundup

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

Contents

Articles	2
Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target US Telecom Networks	2
Vulnerabilities in MongoDB Library Allow RCE on Node.js Servers.....	2
Rhadamanthys Infostealer Being Distributed Through MSC Extension	2
Chinese APT Tools Found in Ransomware Schemes, Blurring Attribution Lines.....	2

Articles

Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target US Telecom Networks

Cisco has confirmed that a Chinese threat actor known as Salt Typhoon gained access by likely abusing a known security flaw tracked as CVE-2018-0171, and by obtaining legitimate victim login credentials as part of a targeted campaign aimed at major U.S. telecommunications companies. An important aspect of the campaign is the use of valid, stolen credentials to gain initial access, although the manner in which they are acquired is unknown at this stage. The threat actor has also been observed making efforts to get hold of credentials via network device configurations and deciphering local accounts with weak password types. Another noteworthy behavior exhibited by Salt Typhoon entails leveraging living-off-the-land (LOTL) techniques on network devices, abusing the trusted infrastructure as pivot points to jump from one telecom to another. Furthermore, Salt Typhoon has been spotted altering network configurations to create local accounts, enable Guest Shell access, and facilitate remote access via SSH. Also put to use is a bespoke utility named JumbledPath that allows them to execute a packet capture on a remote Cisco device through an actor-defined jump-host.

<https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html>

Vulnerabilities in MongoDB Library Allow RCE on Node.js Servers

Two critical-severity vulnerabilities in the Mongoose Object Data Modeling (ODM) library for MongoDB could have allowed attackers to achieve remote code execution (RCE) on the Node.js application server, cybersecurity platform OPSWAT reports. The first of the critical-severity flaws in the library, tracked as CVE-2024-53900, could allow an attacker to exploit the \$where value to potentially achieve RCE on Node.js. The second issue, tracked as CVE-2025-23061, is a bypass for CVE-2024-53900's patch. The cybersecurity organization has released proof-of-concept (PoC) exploit code targeting both vulnerabilities and recommends updating Mongoose to version 8.9.5 or later, which contain complete patches for the two bugs.

<https://www.securityweek.com/vulnerabilities-in-mongodb-library-allow-rce-on-node-js-servers/>

Rhadamanthys Infostealer Being Distributed Through MSC Extension

AhnLab SEcurity intelligence Center (ASEC) has confirmed that Rhadamanthys Infostealer is being distributed as a file with the MSC extension. The MSC extension is an XML-based format that is executed by the Microsoft Management Console (MMC), and it can register and execute various tasks such as script code and command execution, and program execution. There are two types of MSC malware: one exploits the vulnerability of apds.dll (CVE-2024-43572), and the other executes the "command" command using Console Taskpad. The distribution of MSC malware has been on the rise since June 2024, with the type that exploits the vulnerability of apds.dll (CVE-2024-43572) being the most prevalent. The recently discovered MSC file belongs to the type that uses Console Taskpad. The distribution of MSC malware has been on the rise since June 2024. While the type that exploits the vulnerability of apds.dll (CVE-2024-43572) is no longer being executed due to the vulnerability patch, the type that uses Console Taskpad does not exploit the vulnerability, so it can still be used in a normal manner. Thus, users need to be extra cautious when executing MSC files from an unknown source.

<https://asec.ahnlab.com/en/86391/>

Chinese APT Tools Found in Ransomware Schemes, Blurring Attribution Lines

Researchers at Symantec and Trend Micro separately discovered sophisticated tools, once deployed exclusively

for nation-state level cyberespionage, in financially motivated extortion schemes, suggesting deliberate collusion or even the possibility that members of APT groups are moonlighting as ransomware criminals. The attacker used a legitimate Toshiba executable (toshdpdb.exe) to sideload a malicious DLL (toshdpapi.dll) that decrypted a file (toshdp.dat) containing a variant of PlugX — a notorious backdoor known only from previous Chinese cyberespionage operations. Experts point to these overlapping tactics as a disturbing trend. Historically, Chinese espionage operations have not pursued overt financial gain; instead, they have relied on stealth and persistence and long-term data exfiltration. In contrast, Iranian and North Korean threat actors are known to blend cyberespionage with criminal schemes. Technical indicators appear to further reinforce the connection. Multiple anti-malware research units have identified string and code overlap between PlugX and ShadowPad, indicating a close link between the ShadowPad and PlugX developers. Trend Micro also made it clear the malware “is in active development” and the developers are constantly tweaking the code to evade detection and analysis.

<https://www.securityweek.com/chinese-apt-tools-found-in-ransomware-schemes-blurring-attribution-lines/>