



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

13 Feb 25

## Cyber Threat Roundup

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

### Contents

Articles .....	2
Exploitation of Old ThinkPHP, OwnCloud Vulnerabilities Surges .....	2
Google Pays Out \$55,000 Bug Bounty for Chrome Vulnerability .....	2
FINALDRAFT Malware Exploits Microsoft Graph API for Espionage on Windows and Linux .....	2
Sarcoma Ransomware Gang Claims the Theft of Sensitive Data from PCB Maker Unimicron.....	2
DPRK Hackers Dupe Targets into Typing PowerShell Commands as Admin.....	3

## Articles

### Exploitation of Old ThinkPHP, OwnCloud Vulnerabilities Surges

Threat actors have been ramping up the exploitation of two old vulnerabilities in ThinkPHP and OwnCloud, threat intelligence firm GreyNoise warns. The ThinkPHP issue, tracked as CVE-2022-47945 (CVSS score of 9.8), is described as a local file inclusion flaw via the 'lang' parameter. It affects the ThinkPHP framework iterations prior to version 6.0.14 that have the language pack feature enabled. The security defect is not included in US cybersecurity agency CISA's Known Exploited Vulnerabilities (KEV) catalog and has not drawn much attention, although threat actors have been exploiting it in the wild, GreyNoise notes. The OwnCloud bug, tracked as CVE-2023-49103 (CVSS score of 10) and affecting the 'graphapi' app, leads to the disclosure of the PHP environment's configuration details (phpinfo) through a URL in a third-party library. CISA added CVE-2023-49103 to the KEV catalog on November 30, 2023, and warned roughly one year later that it had become one of the top routinely exploited vulnerabilities.

<https://www.securityweek.com/exploitation-of-old-thinkphp-owncloud-vulnerabilities-surges/>

### Google Pays Out \$55,000 Bug Bounty for Chrome Vulnerability

Google on Wednesday announced the rollout of a Chrome browser update that resolves four high-severity vulnerabilities that were reported by external researchers. The first issue is a use-after-free bug in the V8 JavaScript engine, tracked as CVE-2025-0995, which earned the reporting researcher a \$55,000 bug bounty reward. Based on the amount handed out, it is likely that the security defect could be exploited to achieve remote code execution. It is not uncommon for threat actors to target V8 issues in their attacks. The latest Chrome update resolves two other memory safety bugs, namely a use-after-free in Navigation, tracked as CVE-2025-0997, and an out-of-bounds memory access flaw in V8, tracked as CVE-2025-0998. Additionally, it addresses an inappropriate implementation in Browser UI, tracked as CVE-2025-0996. Google notes in its advisory that it has yet to determine the bug bounty amounts to be paid for the last three security defects.

<https://www.securityweek.com/google-pays-out-55000-bug-bounty-for-chrome-vulnerability/>

### FINALDRAFT Malware Exploits Microsoft Graph API for Espionage on Windows and Linux

Threat hunters have shed light on a new campaign targeting the foreign ministry of an unnamed South American nation with bespoke malware capable of granting remote access to infected hosts. The activity, detected in November 2024, has been attributed by Elastic Security Labs to a threat cluster it tracks as REF7707. Some of the other targets include a telecommunications entity and a university, both located in Southeast Asia. The exact initial access vector used in the attacks is currently not clear, although it has been observed that Microsoft's certutil application is used to download additional payloads from a web server associated with the Foreign Ministry.

<https://thehackernews.com/2025/02/finaldraft-malware-exploits-microsoft.html>

### Sarcoma Ransomware Gang Claims the Theft of Sensitive Data from PCB Maker Unimicron

The Sarcoma ransomware group claims to have breached Taiwanese PCB manufacturer Unimicron, leaked sample files, and threatened a full data release if no ransom is paid by Tuesday, February 20, 2025. Unimicron Technology Corporation is a Taiwanese company specializing in the manufacturing of printed circuit boards (PCBs), high-density interconnects (HDI), and IC substrates. It is a key supplier in the semiconductor and

electronics industries, providing critical components for products such as smartphones, computers, automotive electronics, and other high-tech applications. Unimicron is a major supplier for companies like Apple, Intel, and other semiconductor giants, playing a crucial role in global supply chains. The company is headquartered in Taiwan and has manufacturing facilities in multiple countries. Sarcoma ransomware operators claim to have stolen 377 GB of SQL files and documents. Sarcoma has been active since October 2024, and the gang is emerging as a major ransomware group in the threat landscape.

<https://securityaffairs.com/174159/cyber-crime/sarcoma-ransomware-claims-the-theft-of-sensitive-data-from-pcb-maker-unimicron.html>

### **DPRK Hackers Dupe Targets into Typing PowerShell Commands as Admin**

North Korean state actor 'Kimsuky' (aka 'Emerald Sleet' or 'Velvet Chollima') has been observed using a new tactic inspired from the now widespread ClickFix campaigns. ClickFix is a social engineering tactic that has gained traction in the cybercrime community, especially for distributing infostealer malware. It involves deceptive error messages or prompts that direct victims to execute malicious code themselves, often via PowerShell commands. These actions typically lead to malware infections. When executed, the code installs a browser-based remote desktop tool, downloads a certificate using a hardcoded PIN, and registers the victim's device with a remote server, giving the attacker direct access for data exfiltration. Microsoft says it observed this tactic in limited-scope attacks starting January 2025, targeting individuals that work in international affairs organizations, NGOs, government agencies, and media companies across North America, South America, Europe, and East Asia.

<https://www.bleepingcomputer.com/news/security/dprk-hackers-dupe-targets-into-typing-powershell-commands-as-admin/>