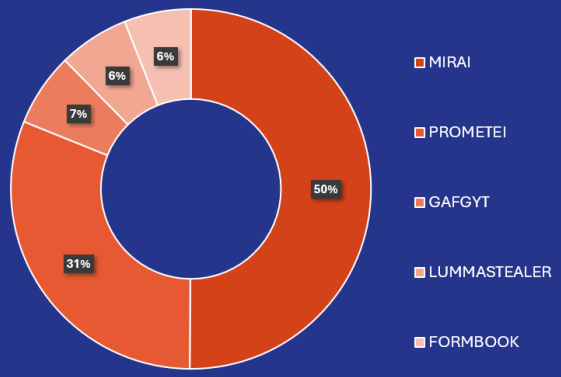
ZENDATA CYBER SECURITY

DEFCON LEVEL

May 2025

The threat alert level has remained unchanged from last month due to ongoing attack campaigns and persistent threat actors.

Most Active Malware



Recent Events

A recent cyberattack has targeted an IT service provider in Switzerland using the LockBit 4.0 ransomware variant. The attackers succeeded in breaching the company's systems, leading to the compromise of stored data. However, their efforts were partially thwarted, preventing the full execution of the attack. Despite this disruption, multiple systems were affected, and client organizations experienced varying degrees of impact. The incident has prompted an ongoing investigation to assess the extent of the damage and identify the perpetrators.

TOP THREAT: UNC6108

UNC6108 is a distribution threat cluster that has used fake Cloudflare verification-themed lures to distribute malware since at least January 2025. These lures leverage the ClickFix social engineering technique and urge the user to copy and paste a mshta command that ultimately leads to the retrieval and execution of a malicious MSI.

TOP VECTOR: PROMETEI

PROMETEI is a botnet backdoor written in C++ that communicates via HTTP and acts as the core component in the PROMETEI modular system. Supported backdoor commands include keyboard and mouse control, shell command execution, file transfer and execution, clipboard manipulation, system information collection, and self-update .

Recent Critical Vulnerabilities

CVE-2025-32433

It is a high-risk vulnerability affecting the Erlang/OTP SSH server. The flaw arises from missing authentication checks during the SSH message handling phase—specifically, in the processing of SSH_MSG_CHANNEL_REQUEST messages. This allows a remote, unauthenticated attacker to send a specially crafted request containing an exec command.

CVE-2025-31324

It is a critical vulnerability affecting SAP NetWeaver Visual Composer's Metadata Uploader component, which allows unauthenticated remote attackers to upload and execute arbitrary JSP files. The flaw stems from a lack of proper authorization on the /developmentserver/metadatauploader endpoint, enabling attackers to send malicious file uploads.

Monthly Recommendations

To mitigate the impact of ransomware attacks like the recent LockBit 4.0 incident, organizations should implement strong network segmentation, ensure regular and secure data backups, deploy advanced endpoint detection and response (EDR) tools, and apply security patches promptly.

To mitigate the risk associated with CVE-2025-32433, it is advised to:

- Disable the SSH server in Erlang/OTP if it is not strictly necessary for your application.

- Restrict SSH access using firewall rules or allowlisting (e.g., only permit trusted IP ranges to access the SSH port).