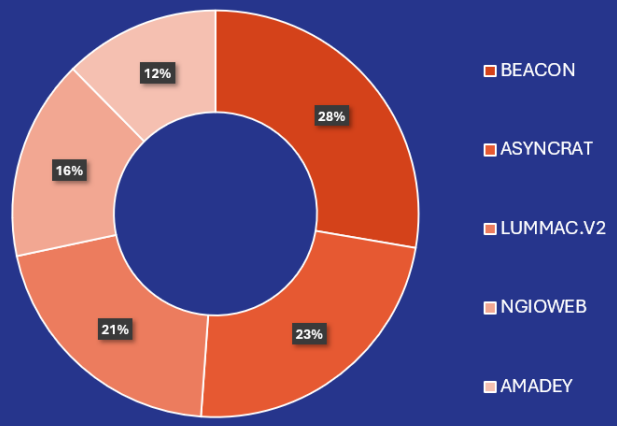
ZENDATA CYBER SECURITY

DEFCON LEVEL

December 2024

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

Most Active Malware



Recent Events

There have been recent reports of Business Email Compromise (BEC). As these emails are sent to customers from businesses through communication channels that include information like: project enquiries and processing, order placement, payment and delivery terms—it makes it an attractive target for scammers to exploit as the damage can be enormous to victims. BEC attacks are financially motivated. Attackers are sophisticated in their methods—after gaining access to the email account, they register domains that look similar to real companies domains.

TOP THREAT: UNC5840

UNC5840 is a financially motivated threat cluster that has obtained access to victim environments via infected USB devices configured to run a multistage dropper. The group's targeting appears to be opportunistic in nature with the end goal of installing and executing cryptocurrency mining software. Over the past month, he has been seen targeting entities in the Government,

TOP VECTOR: CUTFAIL

CUTFAIL is a dropper written in C++ that has been observed to drop multiple files and an encrypted configuration file, as well as various third-party libraries, such as OpenSSL, libcurl, and WinPthreadGC. CUTFAIL launches HIGHREPS and establishes persistences via Windows Service.

Recent Critical Vulnerabilities

CVE-2014-6271

An Input Validation vulnerability exists that, when exploited, allows a remote attacker to execute arbitrary code. This vulnerability has been confirmed to be exploited in the wild, An attacker could use this vulnerability to get complete access to the exploited system or cause bash– to crash. Resulting in denial-of-service. It is a critical risk vulnerability.

CVE-2024-50623

There is an active exploit in the wild for a critical security vulnerability in Cleo file transfer software products. An unrestricted upload of a file with a dangerous type vulnerability exists, when exploited, allows a remote attacker to execute arbitrary code. Due to the potential for arbitrary code execution, it is considered a critical risk vulnerability.

Monthly Recommendations

To reduce the risk of attacks from improper input validation, organizations should practice validating input at multiple layers of web applications. Validation should be applied at different stages such as client-side, server-side and database validation. Adopting principle of least privilege is also good practice. It limits database permission so that even if an attack succeeds, it only has minimal access to data.

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Also to avoid Unrestricted Upload of File with Dangerous Type, organizations can restrict the allowed file types and validate them on the server before uploading.