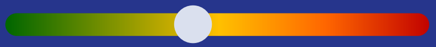
ZENDATA CYBER SECURITY

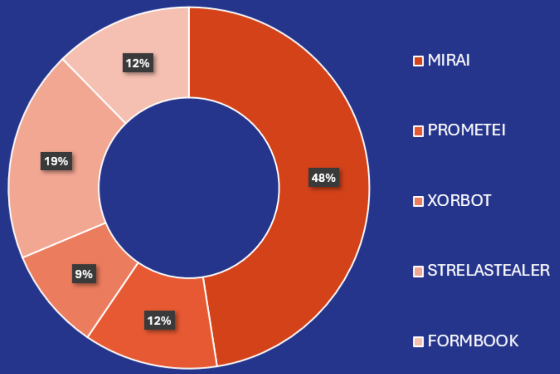
DEFCON LEVEL

January 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

Recently, CEO fraud crimes have been targeting Swiss municipalities. Fraudsters are posing as employees of the audit and consulting company Forvis Mazars. The attackers obtain information about the company from various sources beforehand. There have been reports of cases where people have been approached by email and by phone to trigger payments for a confidential transaction. Emails from alleged CEO to the finance department or from the alleged chairman of an association to the treasurer are used. A credible story is used to persuade the person contacted to make allegedly urgent payments. In this scheme, scammers impersonate Forvis Mazaars' executives' identities and their email addresses to secure unlawful gain.

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 multi-stage dropper, DIRTYBULK, leading to execution of PUMPBENCH backdoor. UNC5840 is conducting a campaign that is leading to installation of PUMPBENCCH backdoor and XMRIG cryptominer software in organizations in Switzerland.

TOP VECTOR: MIRAI

MIRAI is a type of malware that primarily targets Internet of things (IoT) devices to turn them into bots for a botnet. It exploits weak or default passwords to gain control of devices, allowing attackers to carry out DDoS attacks, Notorious for taking down high-profile websites. It is important to secure IoT devices by changing default passwords and regularly update software.

Recent Critical Vulnerabilities

CVE-2024-55591

An Authentication Bypass using an Alternate Path or Channel vulnerability exists in FortiOS & FortiProxy, when exploited, allows a remote attacker to obtain unauthorized access. it has been confirmed to be exploited in the wild and weaponized code is widely available. It is a high risk vulnerability due to the potential for unauthorized access.

CVE-2025-0282

A Stack-based Buffer Overflow vulnerability exists that, when exploited, allows a remote attacker to execute arbitrary code. This vulnerability has been confirmed to be exploited in the wild, and proof-of-concept and weaponized code is publicly available. It is considered a high-risk vulnerability due to the potential for arbitrary code execution.

Monthly Recommendations

To protect against CEO fraud emails, recipients of emails and phone calls urging for payments should proceed with caution. Targets should try to establish contact with the sender through official channels and check email addresses for subtle discrepancies, like misspelled names or altered domains. Avoid clicking on links or opening attachments in they may contain malware or phishing sites.

To protect against CVE-2025-0282 a patch and workaround is suggested. Apply security patch provided by Ivanti immediately. Additionally, limit exposure by disabling unnecessary services or ports, implement network segmentation, and monitor system logs for unusual activity. Regularly update software and conduct vulnerability assessments to prevent future exploitation.