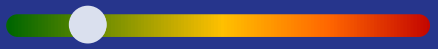
ZENDATA CYBER SECURITY

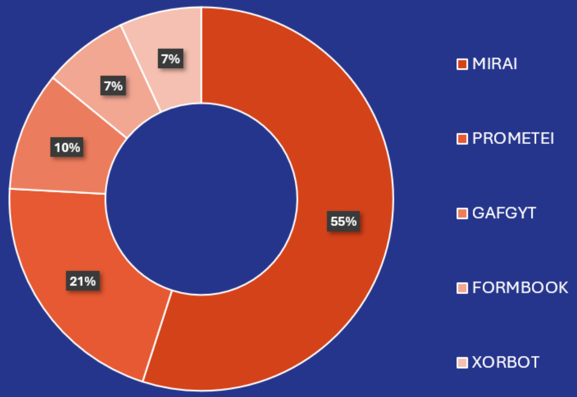
DEFCON LEVEL

March 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

Phishing remains a prevalent scam, with many people falling victim to it. Scammers frequently impersonate trusted brands, including Swiss Post, Swisscom, SBB, and SwissPass, to increase their chances of success. These companies have large customer bases, making them prime targets for phishing attempts. Scammers send mass emails pretending to be from these companies, knowing they are more likely to reach customers. Those expecting parcels from Swiss Post or needing SwissPass renewals are especially vulnerable. The scam messages are designed to look legitimate, using various tactics to deceive people into revealing personal or financial information.

TOP THREAT: SANDWORM

Sandworm is an advanced and operationally mature threat actor involved in espionage, influence, and attack operations since at least 2009. The group conducts disruptive and destructive attacks using wiper malware, focusing on espionage globally. It has a highly extensive operational reach.

TOP VECTOR: PROMETEI

Prometei is a credential stealer written in C that targets Windows authentication credentials. Techniques employed include stealing password hashes, keys and Kerberos tickets. Credentials can be printed to the console or saved to disk. Prometei also supports privilege escalation, extracting credentials from the LSASS, SAM, and service manipulation.

Recent Critical Vulnerabilities

CVE-2025-26465

A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key.

CVE-2025-0108

An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts, it can negatively impact integrity and confidentiality of PAN-OS.

Monthly Recommendations

Be cautious when asked for personal information via email, text, or phone. Always visit websites through official links and avoid entering sensitive data from links in messages. If you suspect that you have entered information on a phishing site, change your passwords immediately. Report phishing sites to www.antiphishing.ch.

The PAN-OS authentication bypass risk is highest if the management interface is exposed to the internet or untrusted networks. Reduce the risk by restricting access to trusted internal IPs. To identify affected devices, review the Customer Support Portal’s Assets section for devices tagged ‘PAN-SA-2024-0015’ needing remediation.