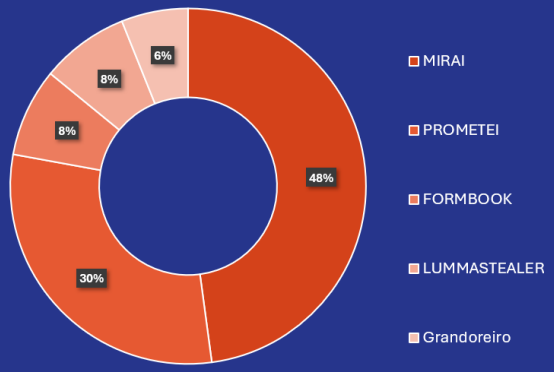
ZENDATA CYBER SECURITY

DEFCON LEVEL

April 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

With festival season and Eurovision ticket sales underway in Switzerland, ticket scams are on the rise. Fraudsters exploit high demand by selling fake or overpriced tickets through **social media and fraudulent websites**. Some steal QR codes from legitimate sellers, while others use **dating apps to direct victims** to fake ticket platforms designed to steal credit card details. Many unknowingly share personal information, later used for fraud. Scammers also create urgency, pressuring buyers into quick decisions. These deceptive tactics make it increasingly difficult to distinguish **genuine offers from scams**, putting Swiss spectators at risk of financial loss and disappointment.

TOP THREAT: Storm0300

Storm0300 is a financially motivated threat cluster that has obtained access to victim networks via CORNFLAKE infections downloaded from phishing sites. The actors have used CORNFLAKE to download and run a variety of secondary payloads, including POSTFLOP, SKYHART, and CHRGETPDSI. It includes activity associated with a former RHYSIDA affiliate, "Clighang."

TOP VECTOR: Mirai

Mirai is a notorious IoT botnet malware that infects unsecured devices like routers and cameras, turning them into bots for large-scale **DDoS attacks**. It spreads by exploiting weak/default credentials. First discovered in 2016, Mirai's source code was leaked, leading to multiple variants and ongoing cyber threats.

Recent Critical Vulnerabilities

CVE-2025-30066

This **Embedded Malicious Code** vulnerability allows remote attackers to steal sensitive information via an **exposed web application**. Exploitation has been reported in the wild, though unconfirmed. Weaponized code is publicly available, increasing risk. A **patch is available** and should be applied to mitigate potential **information disclosure** threats.

CVE-2025-30154

An **Embedded Malicious Code** vulnerability in **reviewdog/action-setup@v1**. Attackers modified the action's script to **extract and leak secrets** from **GitHub Actions Workflow Logs**. Any workflow using this action unknowingly exposed sensitive credentials, affecting other **reviewdog** actions and compromising CI/CD pipeline security.

Monthly Recommendations

Only buy tickets from **official event websites or authorized resellers**. Avoid deals on social media or third-party sites, especially those creating urgency. Never share personal details or ticket QR codes. Use **secure, traceable payment methods**. If scammed, report it to **local authorities and the platform** where the fraud occurred.

Immediately **remove or update affected components** to a secure version. **Rotate any exposed secrets** to prevent unauthorized access. **Restrict access to GitHub Actions Workflow Logs** and monitor for suspicious activity. Implement **least privilege principles** for CI/CD workflows, and regularly **audit dependencies** for potential supply chain compromises.