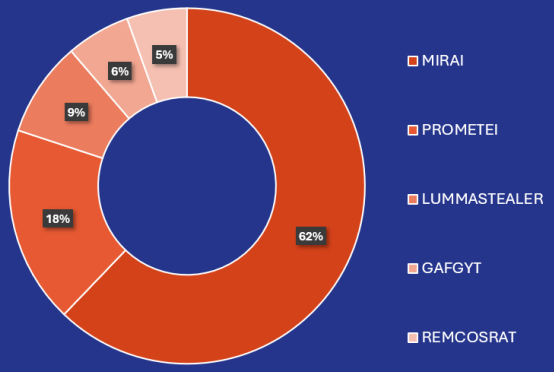
ZENDATA CYBER SECURITY

DEFCON LEVEL

June 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

Cybercriminals are sending alarming emails claiming antivirus subscriptions have expired or accounts are at risk. These messages direct recipients to fake virus scans that always report infections, then redirect to legitimate antivirus websites. The scammers' goal is not to infect devices but to earn commissions from software purchases made through their links. By exploiting fear and urgency, this tactic pressures victims into buying antivirus products while operating in a legal grey area.

TOP THREAT: Sandworm Team

Sandworm Team is a highly skilled cyber threat group active since 2009. They have focused heavily on Ukraine, carrying out disruptive and destructive attacks using malware over the past decade. Beyond this region, they conduct espionage globally, targeting various sectors.

TOP VECTOR: Mirai

Mirai is malware that targets Internet of Things (IoT) devices, turning them into a botnet for large-scale DDoS attacks. Discovered in 2016, it exploits default credentials to infect devices. Mirai variants have since evolved, and the malware's source code release has led to widespread adoption by cybercriminals and hacktivists alike.

Recent Critical Vulnerabilities

CVE-2025-32756

CVE-2025-32756 is a critical stack-based buffer overflow vulnerability affecting multiple Fortinet products, including FortiMail, FortiNDR, and FortiCamera. It allows remote unauthenticated attackers to execute arbitrary code via specially crafted HTTP requests. Fortinet has confirmed active exploitation, particularly targeting FortiVoice systems.

CVE-2025-31324

CVE-2025-31324 is a critical improper authorization vulnerability in SAP NetWeaver's Visual Composer component, allowing remote attackers to upload & execute malicious JSP webshells via the /developmentserver/metadatauploader endpoint. Active exploitation observed since April 2025. Weaponized code publicly available.

Monthly Recommendations

Exercise caution with unsolicited emails claiming antivirus expiration or account compromise. Do not click embedded links or download attachments. Verify software licenses and account status directly via official vendor portals. Be aware that fake virus scans are used as social engineering tactics to drive fraudulent software sales.

Ensure all affected systems are promptly patched against CVE-2025-32756 and CVE-2025-31324. Monitor network traffic for suspicious activity targeting vulnerable endpoints. Implement strict access controls and validate all input to mitigate exploitation risks. Regularly review logs for indicators of compromise related to these vulnerabilities.