OpenVoiceNews Pakistan

Transparent. Unbiased. Yours.

Pakistan's CERT Alerts 39 Ministries to Cyber Threat

August 11, 2025

— Categories: Crime

The National Cyber Emergency Response Team (CERT) has issued a high-level security alert to 39 ministries and key federal departments, warning of an imminent cyberattack involving the BlueLocker ransomware.

According to an official letter circulated by CERT, the threat could result in permanent data loss, operational disruptions, and the exposure of sensitive government information. The advisory stresses that the ransomware specifically targets Windows-based desktops,

laptops, servers, networks, and cloud storage systems, encrypting files and demanding payment for their release.

The letter was addressed to several top government officials, including the Secretary Cabinet Division, Secretary Interior, Secretary Foreign Affairs, Director General of the National Counter Terrorism Authority (NACTA), Director General of the Federal Investigation Agency (FIA), the National Security Division, the Establishment Division, the Election Commission of Pakistan, the National Assembly Secretariat, and the Pakistan Electronic Media Regulatory Authority (PEMRA).

In addition to these, the alert was sent to critical ministries and regulatory bodies such as the Ministry of Finance, the Ministry of Information Technology & Telecommunication, the National Disaster Management Authority (NDMA), the Oil and Gas Regulatory Authority (OGRA), and the Federal Board of Revenue (FBR). The National Information Technology Board (NITB) was also among the notified organizations.

CERT's advisory outlines immediate actions for all departments to reduce the risk of compromise. These include promptly disseminating the advisory within their organizations, isolating any infected systems from networks without delay, and reporting incidents to the appropriate authorities. Departments have also been urged to ensure that backup systems are functioning and updated, and that all software and security patches are installed.

The BlueLocker ransomware, according to CERT, is designed to lock down targeted systems by encrypting critical files. Once a system is infected, victims receive a ransom demand for decryption keys. Such attacks can severely hinder the operations of government entities, particularly if data recovery measures are not in place.

Cybersecurity experts within the government stress that timely precautions are vital to safeguarding sensitive data and ensuring the continuity of essential public services. Officials have urged all federal institutions to heighten their monitoring and review their network security protocols immediately.

This alert follows a global increase in ransomware incidents, with attackers often exploiting outdated software or weak security configurations. CERT's intervention aims to prevent potential breaches that could compromise Pakistan's critical infrastructure and national security.

By issuing this advisory to multiple high-level offices simultaneously, CERT has underscored the urgency and seriousness of the BlueLocker threat, emphasizing that preventive action is the most effective defence against such cyberattacks.