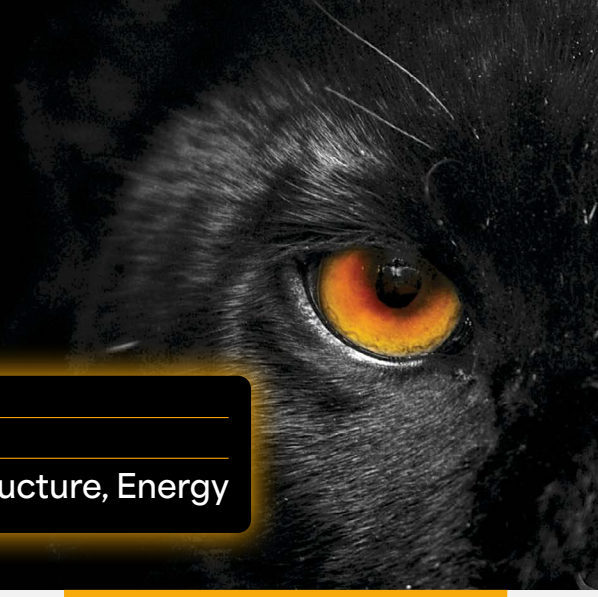
BLACKFOG®

Threat Intelligence Brief



FOCUS	SECTORS
Blue Locker Ransomware	Government, Critical Infrastructure, Energy

Stopping Blue Locker Ransomware: BlackFog's Prevention-First Defense

Understanding Blue Locker

Blue Locker is a high impact ransomware strain that targets Windows-based endpoints such as desktops, laptops, servers, and connected storage systems. It encrypts files with a ".blue" extension (e.g. file.doc.blue) and leaves a restore_file.txt ransom note in each folder, instructing victims to contact the attackers (via ProtonMail) in exchange for a decryption key. The malware is capable of disabling antivirus software, conducting lateral movement, and exfiltrating sensitive data while spreading across networks.

Threat Landscape in Pakistan

NCERT has issued a high priority advisory to 39 government ministries and institutions, warning of a "severe risk" stemming from active Blue Locker operations. The alert follows confirmed attacks on entities such as Pakistan Petroleum Limited (PPL), whose IT infrastructure was significantly disrupted, with the incident resulting in encrypted servers, backups deleted, and financial operations suspended for days. Blue Locker actors are observed to use trojanized downloads, phishing emails, compromised websites, and unsecured file sharing platforms to distribute the malware.

> "Blue Locker actors are observed to use trojanized downloads, phishing emails, compromised websites, and unsecured file sharing platforms to distribute the malware."

How BlackFog Counters Blue Locker

Real-Time Data Protection: BlackFog's anti data exfiltration technology (ADX) prevents outbound data transfers, even those initiated during ransomware encryption processes, protecting data even if encryption begins.

Behavioral & Process Anomaly Detection: Sophisticated behavioral AI flags abnormal file renaming (e.g., .blue suffix additions), scheduled deletion of shadow copies, and mass file encryption events, enabling immediate containment.

BlackFog vs Interlock Ransomware

Threat Vector	Blue Locker Tactic	BlackFog Countermeasure
File Encryption	.blue extension files and ransom note restore_file.txt	File activity detection + ADX-enabled blocking
Antivirus Evasion	Disables security tools	Real-time process monitoring stops illegal process execution
Lateral Spread	Network-wide propagation, backup deletion	Network segmentation and encrypted data channel monitoring
Attack Delivery	Phishing, downloads, compromised websites	Email/Web filter integration + user behavior alerts
Operational Impact	Shuts down financial and mission-critical systems	Rapid containment + process isolation framework

Advisory Recommendations from NCERT

- **Apply Security Patches Promptly** to all systems and software.
- **Enable Multi-Factor Authentication (MFA)** for all user accounts.
- **Strengthen Email and Web Filtering** to block malicious content.
- **Train Staff** on threat identification and avoidance of suspicious downloads.
- **Maintain Offline Backups** of critical data and ensure backups are disconnected during incidents.
- **Preserve Forensic Artifacts** to aid in investigations and incident response.

BLACKFOG®

Why BlackFog?

In a cyber landscape increasingly shaped by human-operated threats, organizations need more than reactive alerts, they need 24/7 real-time prevention. BlackFog delivers exactly that.

With its unique anti data exfiltration (ADX) technology, AI based behavioral threat detection, and dynamic blocking capabilities, BlackFog helps organizations prevent breaches by ensuring unauthorized data never leaves the network.

For organizations with lean internal teams, BlackFog's vCISO services provide expert leadership, streamlined incident response, and compliance-ready reporting, all tailored to the demands of that specific industry.

Ready to Learn More?

Visit blackfog.com or contact us at sales@blackfog.com

Award-winning Technology

MSP Today Product of the Year 2025 · Cybersecurity Breakthrough Award · Fortress Cyber Security Award · teiss Awards 2025 · Globee Awards · Cyber Security Excellence Awards Winner

Follow us:

Android · Chrome · Windows · Apple · iOS

Contact us for a demo

Start your free trial

Visit blackfog.com