A recently-issued joint advisory by the FBI, the Cybersecurity and Infrastructure Security Agency, the Financial Crimes Enforcement Network, and the Treasury Department warns that MedusaLocker ransomware “targets vulnerabilities in Remote Desktop Protocol (RDP) to access victims’ networks.” The alert encourages “network defenders to examine their current cybersecurity posture and apply the recommended mitigations,...including:

- Prioritize remediating known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.”

MedusaLocker exploits vulnerabilities in RDP, encrypts the victim’s data, and sends a ransom note embedded in the encrypted files demanding payment in Bitcoin to obtain the encryption key.
The alert (linked here) provides technical details and mitigation steps.

Source URL: https://www.natlawreview.com/article/joint-advisory-warns-medusalocker-ransomware