Leakware - What it is, how it works, and how to respond

Gridinsoft Help Center

What it is

Leakware is a ransomware tactic that steals sensitive data and threatens to publish it unless you pay. Instead of encrypting files, attackers use exposure as leverage against people and organizations.

How it works - quick tour

- Initial access via phishing, stolen creds, or a vulnerable app
- Discovery and collection of valuable files and mailboxes
- Exfiltration to attacker servers or cloud storage
- Extortion emails and shaming sites announce a countdown to leak

What you may notice

- Sudden logins from unknown locations or unusual data transfers
- New backup or archiving tools installed without approval
- "Proof of theft" emails linking to a leak site or sample files

If it hits - first moves

- Isolate affected systems and rotate credentials from a clean machine.
- Preserve evidence - logs, notes, samples - and alert legal and leadership.
- Engage incident response to scope data taken and block persistence.
- Notify impacted users and regulators as required - prepare containment messaging.
- Improve egress controls and takedown attempts against leak sites.

Prevent it

- MFA everywhere and least privilege for mail, file shares, and VPN
- Patch internet-facing services fast and monitor for data exfiltration
- Encrypt sensitive data at rest and label it for tighter access
- Use EDR/XDR plus DNS/web filtering to spot staging and upload spikes
- Keep offline, tested backups - some actors still encrypt as a second punch