Five early warning signs of a ransomware intrusion, before encryption begins



Acronis outlines five warning signs that can reveal a ransomware intrusion before encryption or data theft, as attackers typically steal credentials, move laterally and try to disable security controls first.

- Ransomware attacks usually involve activity well before encryption starts.
- Credential theft, lateral movement and attempts to disable security controls are typical early stages.
- Acronis describes five warning signs to help defenders detect intrusions sooner.
- Earlier detection supports containment and protection of critical systems and backups.

Acronis has published guidance on spotting ransomware intrusions at an early stage, reported by

BleepingComputer. The central point is that encryption is rarely the first step. Attackers often spend time stealing credentials, moving between systems and trying to switch off security controls before any files are locked or data is taken.

What the guidance covers

Acronis examines five warning signs that defenders can watch for. The excerpt available to us does not list the five signs, so this item does not describe them individually. The stated aim is to help teams detect intrusions earlier, contain malicious activity and protect critical systems and backups.

Why it matters for regulated institutions

The window between initial access and encryption is the period in which a response is most effective. Activity such as unusual use of accounts, movement across internal systems, or tampering with security tools can indicate an attack in progress. Institutions that monitor for these behaviours, rather than waiting for visible damage, have more chance to limit impact.

Security leaders may wish to read the full Acronis guidance and compare its five signs with their own detection coverage. Backups deserve particular attention, since the guidance highlights protecting them alongside critical systems.

Next steps

Treat the pre-encryption stages as a detection priority, confirm that alerts reach people who can act on them, and rehearse containment so that decisions can be taken quickly when early signs appear.

What to do now

1. Read the full Acronis guidance and map its five warning signs to your current detection rules.
2. Monitor for credential misuse and unusual lateral movement between internal systems.
3. Alert on any attempt to disable or tamper with security tools such as endpoint protection.
4. Verify that backups are protected from tampering and that restores are tested.
5. Rehearse a containment playbook for an intrusion detected before encryption.