GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

0-9

3AM Ransomware: Intrusion and Response

What it is 3AM ransomware is a Windows-focused ransomware family observed in attacks against organizations. It can encrypt files, rename affected data with a new extension, and leave a ransom note. Reported operators have also stolen...

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 17, 2026	2 min

What it is

3AM ransomware is a Windows-focused ransomware family observed in attacks against organizations. It can encrypt files, rename affected data with a new extension, and leave a ransom note. Reported operators have also stolen data before encryption, adding the threat of public disclosure to the loss of access.

How it works

An intrusion usually begins before the ransomware runs. Attackers may enter through stolen remote-access credentials or another compromised account, explore the network, disable security tools, and move toward servers and backups. The 3AM payload is then used near the end of the operation to encrypt selected systems and pressure the victim.

Key points

- Unexpected remote logins, disabled endpoint protection, and rapid access to many hosts are more useful early warnings than the ransom note itself.
- Encryption and data theft are separate risks; restoring files does not resolve a possible breach.
- A filename extension alone is not enough to identify a ransomware family with certainty.

What to do

- Isolate affected systems and preserve logs, ransom notes, and a sample of an encrypted file.
- Disable compromised accounts, rotate credentials from a clean device, and review remote-access logs.
- Verify backups before restoration and rebuild systems only after the initial access path is closed.
- Do not run an unknown decryptor on the only copy of affected data.

Investigate what happened before encryption

Preserve the ransom note, extension, executable, first affected host, remote-login records, and data-transfer evidence. Isolate systems, disable compromised accounts, and protect backup administration before restoration. Search for persistence and remote tools on other endpoints because encryption is often a late incident stage. Keep an untouched copy of encrypted data and avoid unverified decryptors. A family name may change or be misidentified, but the response priorities remain the same. Follow the complete ransomware response process for containment, credential rotation, clean rebuilding, and monitoring.