0-9

3AM Ransomware: Identification, Attack Chain, and Recovery Response

3AM is a Rust-based ransomware family identified by the .threeamtime extension and RECOVER-FILES.txt note. Learn the observed intrusion chain and safe incident-response priorities.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How to identify 3AM ransomware
02 The observed 3AM attack chain
03 What to do in the first response
04 Recovery and decryption
05 How to reduce 3AM-style ransomware risk
06 Frequently asked questions

3AM ransomware is a 64-bit Windows ransomware family written in Rust. It was publicly documented in 2023 after an attacker used it as a fallback when an attempted LockBit deployment was blocked. The observed payload encrypted selected files, added the

`.threeamtime` extension, created `RECOVER-FILES.txt` ransom notes, attempted to stop security and backup services, and deleted Windows shadow copies.

Incident priority: the ransomware executable is usually the final impact stage of a broader intrusion. Containing encryption without finding the stolen account, persistence, remote tooling, and possible data theft leaves the organization exposed.

01 How to identify 3AM ransomware

Observed clue	Meaning	Limit
`.threeamtime` extension	Used by the documented 3AM payload	An extension can be imitated
`RECOVER-FILES.txt`	Ransom note placed in scanned folders	Preserve it; do not rely on its claims
Services stop before encryption	May indicate attempts to unlock files or weaken backup/security tools	Service failure has many benign causes
Shadow copies disappear	Local recovery was deliberately impaired	Does not prove which ransomware family acted
Unusual remote administration and discovery	Can reveal the intrusion before encryption	Requires timeline and account context

Confirm the family with the ransom note, file structure, security telemetry, and a malware sample. Do not identify ransomware from the filename extension alone.

02 The observed 3AM attack chain

In the original public case, the attacker performed network and account discovery, used Cobalt Strike components, attempted privilege escalation and lateral movement, created a user for persistence, and exfiltrated data with a command-line transfer tool. LockBit was attempted first; after it was blocked, the attacker switched to 3AM.

1. **Existing access:** the operator controls an account or host before 3AM runs.
2. **Discovery:** commands enumerate users, policies, sessions, shares, and reachable servers.
3. **Privilege and movement:** remote tools and administrative access extend control.
4. **Data theft:** selected files may leave the network before encryption.
5. **Defense and recovery impairment:** services, logs, backups, or recovery settings are targeted.
6. **Encryption:** 3AM encrypts matching files and creates ransom notes.

This ordering explains why a clean decryptor, even if one becomes available, would solve only the file-access problem and not the breach.

03 What to do in the first response

1. **Isolate affected systems.** Disconnect network access at the switch, EDR, or virtualization layer when practical. Do not power off every host automatically; memory and live connections can be important evidence.
2. **Protect backups and administration.** Restrict backup consoles, hypervisors, identity systems, and remote-management tools using clean accounts.
3. **Disable confirmed compromised accounts.** Revoke sessions and rotate credentials from a trusted device, prioritizing administrators, service accounts, VPN, and backup access.
4. **Preserve evidence.** Save ransom notes, encrypted samples, security alerts, authentication logs, process data, network records, and the first-known affected host.
5. **Block known activity carefully.** Quarantine confirmed payloads and malicious infrastructure, but retain samples needed for analysis.
6. **Engage incident-response, legal, and privacy teams.** Data exfiltration may create notification obligations independent of encryption.

04 Recovery and decryption

Do not assume that a public 3AM decryptor exists for the exact variant. Check reputable ransomware-recovery initiatives and security vendors using a copy of the ransom note and encrypted sample. Avoid tools supplied by anonymous accounts or attackers.

Restore only after the initial access path and persistence have been removed. Build clean systems, patch the exploited weakness, rotate credentials, validate backups offline, and restore in a staged network. Monitor the rebuilt environment for re-entry and delayed activity.

Should an organization pay?

Payment does not guarantee a working decryptor, deletion of stolen data, or protection from another demand. It can also create legal or sanctions risk. Involve leadership, legal counsel, insurers, and law enforcement; do not let an individual administrator negotiate from the affected network.

05 How to reduce 3AM-style ransomware risk

- require MFA for remote and privileged access and remove unused accounts;
- separate workstation, server, backup, and administrative credentials;
- keep immutable or offline backups and test full restoration;
- alert on new administrators, unusual remote tools, mass service stops, log clearing, and shadow-copy deletion;
- segment critical servers and restrict east-west administrative protocols;
- retain endpoint, identity, firewall, VPN, and backup logs long enough to reconstruct the pre-encryption activity.

06 Frequently asked questions

Is 3AM the same as LockBit?

No. They are different ransomware families. A documented affiliate attempted LockBit and then used 3AM after LockBit was blocked, showing that the same operator may switch payloads.

Does restoring files finish the incident?

No. Investigate credential theft, persistence, lateral movement, and exfiltration before declaring recovery complete.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com