GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

T

Trigona Ransomware: Incident Response

What it is Trigona is a Windows ransomware family used in attacks against organizations. Operators encrypt data and demand payment, and public reporting has associated some incidents with poorly protected or exposed services, including...

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

What it is

Trigona is a Windows ransomware family used in attacks against organizations. Operators encrypt data and demand payment, and public reporting has associated some incidents with poorly protected or exposed services, including database servers. The family name comes from imagery and branding used in its ransom materials.

How it works

Attackers first gain access, identify valuable systems, and obtain the privileges needed to reach data and backups. The ransomware then encrypts selected files and leaves instructions for contacting the operator. Exact initial access can vary, so an exposed SQL service should be investigated as one possible path rather than assumed in every case.

Key points

- Internet-facing databases should never rely only on a password and broad network exposure.
- The visible encryptor does not reveal whether data was collected or other access methods remain.
- Extension and ransom-note details help identification but should be verified with technical evidence.

What to do

- Isolate affected hosts and remove public exposure from unnecessary database and remote services.
- Preserve logs from databases, firewalls, identity systems, and endpoints before rebuilding.
- Rotate credentials, repair the entry path, and protect backups from compromised accounts.
- Restore only after clean systems and tested backup copies are available.

Do not stop at the encrypted files

Record the ransom note, extension, affected shares, first observed host, and remote-login evidence before rebuilding. Isolate systems, disable compromised accounts, and protect backup consoles and hypervisors. Review data-transfer activity because encryption may follow collection and theft. Keep an untouched copy of encrypted files, but do not assume a tool labeled for Trigona is legitimate or compatible with every variant. Recovery starts after the access path and persistence are removed. Follow the broader ransomware response guide for evidence preservation, notification decisions, clean restoration, and monitoring.