T

Trigona Ransomware: Identification and Response

Trigona was a Windows ransomware operation associated with organizational attacks and compromised MSSQL servers. Learn what evidence identifies it, why initial-access investigation matters, and how to contain and recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How Trigona attacks unfolded
02 Evidence to preserve
03 Immediate containment
04 Recovery
05 How to reduce the risk
06 Frequently asked questions

Trigona is a Windows ransomware family and operation that emerged publicly in 2022. Trend Micro tracked the operators as Water Ungaw and documented attacks against organizations, including campaigns targeting compromised Microsoft SQL Server (MSSQL) systems through password brute force. The encryptor was only the visible final stage;

responders must also find the initial access and any remaining attacker control.

Public reporting described disruption of Trigona's infrastructure in October 2023. That does not make an old detection or encrypted system harmless, and another actor can reuse a name, note, or sample. Treat current claims as an identification question requiring evidence.

01 How Trigona attacks unfolded

1. **Initial access:** operators used compromised access. In a documented 2023 campaign, exposed MSSQL servers with weak credentials were brute-forced.
2. **Execution and discovery:** commands and tools were used to understand the host and prepare the ransomware stage.
3. **Privilege and reach:** attackers sought access to valuable files, shares, credentials, and systems.
4. **Encryption:** the ransomware encrypted selected data and generated instructions for contacting the operator.
5. **Extortion:** the victim was directed to a negotiation channel. The visible note did not reveal whether other malware or access remained.

Do not assume every Trigona incident began with SQL Server. Phishing, stolen remote credentials, an exploited service, or another foothold may produce similar evidence. Build the timeline from logs.

02 Evidence to preserve

- The ransom note, added file extension, encrypted samples, and any matching original files.
- Security detection names, file hashes, process trees, command lines, services, and scheduled tasks.
- MSSQL authentication, error, audit, and query logs, including failed logins before the first suspicious command.
- Firewall, VPN, remote-access, identity, EDR, DNS, proxy, and cloud logs.

- The first affected host, earliest changed file, accounts used, and reachable shares.
- Outbound transfers and staging archives that may indicate data exfiltration.

Preserve volatile evidence before shutdown when your incident plan and responder support require it. Otherwise prioritize isolation so encryption cannot spread.

03 Immediate containment

1. **Isolate affected hosts** from internal networks and the internet. Disconnect writable backup targets and shared storage.
2. **Remove unnecessary exposure** from MSSQL, RDP, administration panels, and other remote services. Do not leave a database port broadly reachable.
3. **Disable compromised accounts and sessions.** Rotate administrative, database, service, backup, hypervisor, and cloud credentials from clean systems.
4. **Block confirmed indicators** while avoiding unverified broad blocks that disrupt legitimate services.
5. **Hunt across the environment** for the same account use, tools, hashes, commands, persistence, and network destinations.
6. **Preserve evidence** for legal, insurance, regulatory, law-enforcement, and recovery decisions.

04 Recovery

Do not begin mass restoration while the access path or persistence remains active. Rebuild compromised systems from trusted images, patch exposed services, enforce network restrictions, and restore only verified data. Keep untouched encrypted samples in case a legitimate decryption method becomes available, but never run a “Trigona decryptor” from an advertisement or negotiation chat without independent verification.

A decryption tool, if one is available for a specific sample, addresses files—not stolen credentials, backdoors, or data exposure. Follow the broader ransomware response process and test application consistency after restoration.

05 How to reduce the risk

- Place databases behind firewalls or private network access and allow only required source systems.
- Use unique, managed service credentials and MFA for interactive remote administration.
- Disable or rename unnecessary default accounts, rate-limit authentication, and alert on repeated failures.
- Patch SQL Server, Windows, management tools, and internet-facing applications.
- Separate user, server, database, backup, and management networks.
- Use endpoint monitoring and application control on servers, with alerts for shells or scripting tools launched by database services.
- Maintain offline, immutable, or separately administered backups and test clean restoration.

06 Frequently asked questions

Does a Trigona ransom note prove the family?

No. Notes and extensions can be copied. Confirm with file analysis, hashes, process evidence, and a trusted ransomware identification service.

Should an exposed MSSQL server simply be patched and restored?

No. Investigate credentials, commands, persistence, lateral movement, and data transfer first. Rebuild when system integrity cannot be established, then close exposure before restoring service.

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