N

NetWalker Ransomware: How attacks spread and how to respond

What it is NetWalker, also known as Mailto, is a ransomware family and affiliate operation that targeted organizations, including healthcare, education, government, and businesses. Operators encrypted systems and used stolen data as...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

NetWalker, also known as Mailto, is a ransomware family and affiliate operation that targeted organizations, including healthcare, education, government, and businesses. Operators encrypted systems and used stolen data as additional leverage, making incidents both an availability crisis and a potential data breach.

How it works

Attackers used phishing, exposed or weakly protected remote access, and vulnerabilities in internet-facing systems. After entry, they gathered credentials, moved through the network, collected data, and attempted to weaken defenses and backups. The ransomware payload was

deployed after the attackers had positioned themselves for broad impact.

Key points

- Encryption is usually a late-stage event, so earlier identity and remote-access anomalies are critical clues.
- Restoring files does not address data that may have been copied before encryption.
- The NetWalker name is historical, but the same intrusion pattern remains common across ransomware operations.

What to do

- Isolate affected segments and protect backup systems from compromised administrator accounts.
- Disable exposed access paths and rotate privileged credentials before recovery begins.
- Preserve evidence of staging, archive creation, cloud uploads, and lateral movement.
- Rebuild from trusted sources and complete breach assessment and notification as required.