N

NetWalker Ransomware: Identification, Containment, and Recovery

NetWalker, also called Mailto, was ransomware used in targeted intrusions and data-extortion attacks. Learn how to identify evidence, contain the incident, and recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How NetWalker attacks progressed

02 How to identify a possible NetWalker incident

03 Immediate containment

04 Data-theft assessment

05 Recovery options

06 Why paying is risky

07 Prevent similar ransomware intrusions

08 Frequently asked questions

NetWalker, also known as **Mailto**, is a ransomware family and ransomware-as-a-service operation associated with targeted attacks against organizations. Operators combined file encryption with theft of sensitive data, turning an incident into both an availability crisis and a potential data breach.

NetWalker is primarily a historical family name, but affected systems and old evidence still require careful recovery. Similar intrusion methods remain common across current ransomware operations.

01 How NetWalker attacks progressed

1. Attackers gained access through phishing, exposed remote services, stolen credentials, or vulnerable internet-facing systems.
2. They collected credentials, mapped the network, and identified valuable servers, backups, and administrator accounts.
3. Data could be staged and removed before encryption.
4. Security and recovery controls were weakened where possible.
5. The ransomware payload was deployed across selected systems, sometimes using scripts or memory-based execution.
6. Victims received a ransom note and could face threats to publish stolen data.

Encryption is the visible final stage. Earlier identity and network evidence is essential for understanding the full compromise.

02 How to identify a possible NetWalker incident

- A security alert specifically naming NetWalker, Mailto, or associated PowerShell behavior.
- Files suddenly receive an unfamiliar extension and no longer open.
- Ransom notes appear in multiple directories.
- PowerShell or another scripting engine runs encoded or unusual commands from an unexpected parent process.

- Privileged accounts connect to many systems or shared resources outside normal administration.
- Large archives, data-staging directories, or unusual outbound transfers appear before encryption.
- Backups, shadow copies, security tools, or recovery settings are altered.

Extensions and note names can vary. Identify ransomware through multiple artifacts, not one filename copied from an online guide.

03 Immediate containment

1. **Isolate affected systems and network segments.** Disconnect shared storage when it is being encrypted, but avoid wiping systems or destroying volatile evidence.
2. **Activate incident response** and establish secure communications outside the affected environment.
3. **Disable compromised accounts and remote access** while preserving authentication evidence.
4. **Protect backup systems** by restricting access from the compromised domain and rotating backup credentials from clean devices.
5. **Preserve evidence:** ransom notes, encrypted samples, suspicious scripts, process data, event logs, VPN records, identity logs, and transfer history.
6. **Search for the initial access path and other affected hosts** before beginning broad restoration.

04 Data-theft assessment

Restoring encrypted files does not answer whether information was stolen. Review:

- access to file servers, databases, email, cloud storage, and backup repositories;
- creation of large archives and staging folders;
- uploads to cloud services, file-transfer tools, or unusual external hosts;

- access by compromised administrator and service accounts;
- legal, contractual, privacy, and regulatory notification requirements.

Handle data exfiltration as a separate incident workstream even when recovery from backup succeeds.

05 Recovery options

Option	Important limitation
Restore from backup	The backup must be clean, protected from attacker access, and tested before production use.
Use a decryptor	It must support the exact variant and key situation; a tool for another family can damage files.
Rebuild systems	Applications, identity, and configuration must be restored without reintroducing persistence.
File repair or data reconstruction	Partial recovery may be possible from unaffected copies, exports, email, snapshots, or application-level replicas.

Keep untouched copies of representative encrypted files and ransom notes before testing recovery. Use recognized law-enforcement, security-vendor, or established ransomware-recovery projects to check for a legitimate decryptor. Avoid unknown tools and services that demand an advance payment or upload of sensitive data.

06 Why paying is risky

A payment does not guarantee a working key, safe decryptor, complete data deletion, or protection from another demand. It may also create sanctions and legal concerns. Coordinate with legal counsel, insurers, law enforcement, and qualified incident responders.

07 Prevent similar ransomware intrusions

- Patch internet-facing services and remove unused remote-access exposure.
- Require phishing-resistant MFA for VPN, email, cloud, and privileged administration.
- Use separate administrator accounts and restrict lateral movement.
- Monitor scripting, credential access, archive creation, remote tools, and backup-console activity.
- Maintain offline or immutable backups with separate credentials and tested restoration procedures.
- Prepare a ransomware response plan that includes business operations, communications, privacy, legal, and recovery.

08 Frequently asked questions

Are NetWalker and Mailto the same ransomware?

Mailto is an alternate name associated with NetWalker. Researchers and security products may use different labels for samples and activity.

Can NetWalker files always be decrypted?

No. Recovery depends on the exact variant, key handling, available backups, and whether a trusted decryptor exists. Never test an unverified tool on the only copy of encrypted data.

Does removing NetWalker restore files?

No. Removing the executable can stop further malicious activity but does not reverse completed encryption. The broader intrusion, stolen credentials, persistence, and possible data theft must also be addressed.

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