L

Leakware (Doxware): Data-Theft Extortion and Incident Response

Leakware or doxware steals sensitive data and threatens disclosure for payment. Learn how it differs from ransomware, how to assess an extortion claim, and how to respond to a possible breach.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 Leakware vs ransomware and double extortion

02 How a leakware attack unfolds

03 How to assess whether data was really stolen

04 Immediate incident-response steps

05 Legal, notification, and communication issues

06 Should a victim pay?

07 Frequently asked questions

Leakware, also called **doxware** or extortionware, is an attack in which criminals steal sensitive information and threaten to publish, sell, or notify others about it unless the victim pays. The pressure comes from loss of confidentiality. Files do not have to be encrypted for a leakware attack to cause a reportable data breach.

Core response principle: treat the extortion message as an unverified breach claim until evidence establishes what happened, but begin containment and legal assessment immediately. Payment cannot prove that every stolen copy was deleted.

01 Leakware vs ransomware and double extortion

Attack type	Primary pressure	Data access
Traditional ransomware	Systems or files are encrypted	The victim loses availability
Leakware or doxware	Stolen data may be exposed	The victim may still access local files
Double extortion	Encryption plus a disclosure threat	Availability and confidentiality are both affected
Pure data extortion	Attackers claim theft without deploying encryption	Operations may appear normal despite a breach

Modern attackers often use the same intrusion methods for all four outcomes. The absence of encrypted files or a ransom-note extension does not mean there was no extortion incident.

02 How a leakware attack unfolds

1. **Initial access:** phishing, stolen credentials, exposed remote access, a vulnerable public service, or a compromised supplier provides entry.
2. **Discovery:** attackers locate file shares, cloud storage, source repositories, mailboxes, databases, backups, and administrative systems.

3. **Collection:** valuable files are staged in archives or synchronized to a controlled location.
4. **Exfiltration:** data leaves through web storage, file-transfer tools, remote administration, or other channels.
5. **Extortion:** the attacker sends samples, a directory listing, screenshots, or a deadline and threatens publication.

03 How to assess whether data was really stolen

An attacker's sample can be genuine, outdated, purchased from another breach, or mixed with fabricated claims. Do not open files or visit a leak site from a production computer. Preserve the original message and validate evidence in a controlled environment.

- compare sample records with current and historical internal data;
- check whether canary files, unique document versions, or metadata identify the source system;
- review identity, cloud audit, database, VPN, proxy, DNS, firewall, and endpoint logs;
- look for archive creation, unusual synchronization tools, large outbound transfers, or many small downloads;
- identify the first compromised account and the time range, not only the final transfer;
- determine whether the attacker retained persistence after exfiltration.

Missing network logs do not prove that nothing left. Document evidence gaps and base notifications on legal guidance and the best available findings.

04 Immediate incident-response steps

1. **Activate the incident plan.** Include security, IT, legal, privacy, executive, communications, insurer, and relevant business owners.
2. **Contain access without destroying evidence.** Disable confirmed compromised accounts, revoke sessions and tokens, isolate affected hosts, and restrict exposed services.

3. **Protect logs and backups.** Copy audit data to controlled storage and prevent the attacker from deleting evidence or recovery assets.
4. **Preserve the demand.** Keep the message, headers, account identifiers, payment details, claimed samples, and timestamps. Do not negotiate from a compromised mailbox.
5. **Scope the affected data.** Identify record types, owners, jurisdictions, individuals, secrets, and intellectual property involved.
6. **Close the entry path and persistence.** Patch exploited systems, rotate credentials, remove malicious accounts and tools, and rebuild untrusted hosts.

05 Legal, notification, and communication issues

Breach-notification duties depend on the data, affected people, contracts, industry, and jurisdictions. Contact qualified legal and privacy counsel early. Law enforcement and national cyber authorities may provide reporting channels and intelligence. Preserve privilege where applicable and keep a decision log.

Communicate confirmed facts, actions, and practical guidance. Do not repeat the attacker's claims as established truth or promise that copied data has been deleted. If credentials, tokens, or identity documents were exposed, give affected people specific reset and monitoring steps.

06 Should a victim pay?

Payment does not guarantee deletion, silence, accurate scoping, or protection from resale and a second demand. It may also create legal or sanctions issues. Any decision should involve leadership, counsel, insurers, and law enforcement rather than an individual technical responder.

07 Frequently asked questions

Is leakware always malware?

The term can describe the extortion tactic even when attackers use stolen credentials and legitimate cloud tools instead of a distinct malware executable.

Can backups solve leakware?

Backups restore availability but cannot retrieve copies already stolen. The response must address confidentiality, notification, credentials, and persistent access.

Does a screenshot prove a full breach?

It proves only that the attacker obtained or accessed what is shown, if authentic. Establish the source, date, scope, and transfer evidence before accepting broader claims.

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