R

REvil (Sodinokibi) Ransomware: Attack Chain and Response

REvil, also called Sodinokibi, was a major ransomware-as-a-service operation. Learn how incidents varied and how defenders should investigate and recover.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What was REvil?
02 Why the Kaseya incident matters
03 Typical attack objectives
04 Evidence to collect
05 Immediate response
06 Reducing ransomware risk
07 Frequently asked questions

Quick answer: REvil, also called Sodinokibi, is a ransomware family and the name commonly applied to the ransomware-as-a-service operation that used it. The core operators supplied malware and extortion infrastructure, while affiliates conducted

intrusions. As a result, access methods and tools differed from case to case. A sound response must follow the evidence in the affected environment rather than rely on one “REvil attack pattern.”

01 What was REvil?

REvil became prominent in 2019 and was used in high-impact attacks against organizations. Its RaaS structure divided work between developers/operators and affiliates who obtained access, moved through networks, stole data, and deployed the payload. It is also known as Sodinokibi or Sodin. Those names can refer to the malware, the service, or the actors in reporting, so incident documentation should state exactly what the label describes.

Public activity and infrastructure have changed over time, and law-enforcement actions disrupted parts of the operation. That history does not make an old REvil binary harmless, nor does it mean that every current ransomware incident using similar techniques is REvil. Attribution is secondary to containment.

02 Why the Kaseya incident matters

In July 2021, malicious actors used Kaseya VSA software and affected managed service providers and their customers. This is a well-known REvil example because one upstream compromise created downstream impact at many organizations. A joint holiday and weekend ransomware advisory from CISA and the FBI cites the Sodinokibi/REvil incidents affecting both a food producer and remote-management implementations.

The lesson is not that all REvil attacks came through Kaseya. Other reported entry paths included stolen credentials, exposed or vulnerable remote services, phishing, and access acquired from other criminals. Defenders should check current vendor advisories and their own logs before deciding how access occurred.

03 Typical attack objectives

1. **Gain and expand access:** compromise an account or system, elevate privileges, and identify domain, virtualization, backup, and security infrastructure.
2. **Steal data:** collect valuable business information and transfer it outside the network for added extortion pressure.
3. **Reduce recovery options:** interfere with security controls, snapshots, or reachable backups when permissions allow.
4. **Encrypt and extort:** encrypt local and network data, leave instructions, and threaten publication of stolen material.

Not every incident completes every stage. Early discovery may prevent encryption, but the organization must still assess whether credentials or data were exposed.

04 Evidence to collect

- the ransom note, encrypted-file samples, extension, executable hash, signature, and process tree;
- authentication events, new or changed accounts, privilege use, and remote-service activity;
- endpoint alerts, scheduled tasks, services, scripts, and attempts to stop security or backup processes;
- network connections and unusual transfers from file servers or cloud repositories;
- administrative actions in MSP, RMM, virtualization, identity, and backup consoles.

Preserve original evidence and record times in a consistent time zone. A ransom-note style or filename can suggest a family, but identification should combine several independent artifacts. Old lists of IP addresses and hashes age quickly.

05 Immediate response

1. **Isolate affected hosts and network segments.** Stop propagation while preserving systems needed for investigation.
2. **Protect identity systems.** Disable confirmed compromised accounts, revoke sessions, and rotate privileged, service, API, and backup credentials from a clean administrative workstation.
3. **Secure management planes.** Review RMM, MSP, hypervisor, domain, and backup consoles for unauthorized access or configuration changes.
4. **Find patient zero and the dwell period.** Determine the earliest confirmed access and hunt across the environment for related activity.
5. **Assess exfiltration and obligations.** Identify exposed data and involve legal, privacy, insurance, law enforcement, and communications teams as appropriate.
6. **Rebuild and restore.** Eradicate persistence, close the entry path, rebuild systems whose integrity is uncertain, and restore tested clean data in priority order.

Do not reconnect restored systems to an environment where attacker access remains active. Payment does not guarantee working decryption, deletion of stolen data, or freedom from legal restrictions; it should never replace incident recovery and specialist advice.

06 Reducing ransomware risk

Use phishing-resistant MFA for privileged and remote access, minimize exposed management interfaces, and patch actively exploited vulnerabilities rapidly. Separate administrative accounts from normal email and browsing, segment endpoints from critical servers, restrict service-account privileges, and centralize tamper-resistant logs. Maintain offline or logically isolated backups and test full restoration, not merely backup completion.

Organizations relying on MSP or remote-management platforms should inventory which tenants can execute software, enforce MFA and least privilege, monitor global actions, and maintain an emergency method to disable integrations. Supply-chain resilience is part of ransomware defense.

07 Frequently asked questions

Are REvil and Sodinokibi the same?

They are widely used as names for the same ransomware family and associated operation, although reports may use the labels at different levels.

Did REvil attacks always use Kaseya?

No. The Kaseya VSA incident was an important supply-chain event, but affiliates used multiple access paths.

Can a decryptor replace incident response?

No. Even successful file decryption does not remove persistence, revoke stolen credentials, explain data theft, or close the original access path.

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