B

BabLock Ransomware: Naming, Evidence, and Response

BabLock is a name used in some security reporting for ransomware associated with the Rorschach family. Learn why naming is inconsistent, what evidence to preserve, and how to contain and recover without trusting an unverified decryptor.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What a detection tells you

02 How BabLock/Rorschach reporting describes the attack

03 Evidence to preserve

04 Immediate response

05 Decryption and recovery cautions

06 Prevention priorities

07 Frequently asked questions

BabLock is a name used by some security vendors and detection systems for ransomware associated with reporting on the **Rorschach** family. Malware naming is not uniform: the same or related sample can receive a vendor detection, an internal builder name, and a research name. A “BabLock” alert should therefore begin an evidence-based identification process, not trigger assumptions about one extension, operating system, or decryptor.

Check Point Research publicly described Rorschach in 2023 as a fast Windows ransomware with defense-evasion and anti-analysis features. Other researchers have used BabLock as an alternate label. This does not mean every file named BabLock is identical or that compatibility with any recovery tool is guaranteed.

01 What a detection tells you

A ransomware detection indicates code or behavior associated with file encryption or an extortion campaign. It does not by itself establish:

- How the attacker entered the environment.
- Whether the encryptor executed successfully.
- Which accounts or systems the attacker controlled.
- Whether data was stolen before encryption.
- Whether backups, hypervisors, or security tools were accessed.
- Whether a public decryptor supports the exact sample.

02 How BabLock/Rorschach reporting describes the attack

Published analysis of Rorschach documented Windows-focused enterprise deployment, rapid encryption, and techniques intended to evade analysis and security controls. Some incidents used legitimate or signed components for DLL sideloading, in which a trusted program loads a malicious library. Researchers also documented domain-wide deployment methods in an affected environment.

These details are useful hunting hypotheses, not a checklist that every BabLock-labeled sample must follow. Confirm file hashes, process trees, loaded modules, command lines, and deployment evidence.

03 Evidence to preserve

- The complete security detection name, engine, timestamp, file hash, and path.
- Ransom note, added extension, encrypted samples, and any matching original file.
- Process trees, loaded DLLs, command lines, services, tasks, and remote-execution evidence.
- Authentication, directory service, EDR, firewall, VPN, DNS, proxy, file-server, backup, and hypervisor logs.
- The first affected host and account, earliest modified files, and reachable shares.
- Large archives or outbound transfers that could indicate data theft.

04 Immediate response

1. **Isolate affected hosts** and stop access to shared storage. Protect backup systems from compromised accounts.
2. **Disable suspected accounts and sessions** while retaining authentication evidence.
3. **Preserve volatile and disk evidence** according to the organization’s incident plan before destructive cleanup.
4. **Scope the intrusion** across endpoints, servers, identity, administration, and remote-access systems. Hunt for DLL sideloading and deployment tools, but do not limit the search to them.
5. **Determine the entry path** and repair it before restoration: exposed service, stolen credential, phishing, vulnerable application, or another foothold.
6. **Rebuild compromised systems** from trusted images and rotate administrative, service, backup, and application secrets from clean systems.
7. **Restore verified backups** only after the environment is clean and segmented.

05 Decryption and recovery cautions

Keep untouched encrypted originals. Search recognized ransomware identification and law-enforcement resources using the note, sample, and extension, but do not trust a tool merely because its page mentions BabLock or Rorschach. Verify the publisher, signature, supported variant, and instructions; test duplicate data first.

A working decryptor restores some files but does not remove persistence, close attacker access, rotate stolen credentials, or address notification duties. Follow the full ransomware response lifecycle.

06 Prevention priorities

- Use phishing-resistant MFA and restrict remote administration.
- Patch exposed systems and segment user, server, management, and backup networks.
- Limit domain-wide software deployment and service-account privileges.
- Monitor unusual remote execution, library loading, security-tool tampering, and mass file changes.
- Maintain immutable or offline backups under separate administrative control and test restoration.

07 Frequently asked questions

Are BabLock, Rorschach, and Babuk the same?

No. Some reporting associates BabLock with Rorschach naming, while Rorschach researchers noted similarities with multiple families and possible reuse of ideas from leaked Babuk code. Similarity or borrowed code does not make all three names interchangeable.

Does BabLock infect Linux?

Do not assume platform support from a generic article or note. Public Rorschach analysis focused on Windows. Identify the actual executable format and affected systems for the specific incident.

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