GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

C

Cryptovirology: How Malware Uses Cryptography and How to Respond

Cryptovirology studies malicious uses of cryptography, including extortion, concealment, information theft, and asymmetric control. Ransomware is one prominent application.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

Cryptovirology studies how cryptographic techniques can be used to create or strengthen malicious software. Cryptography normally protects confidentiality, integrity, and authentication; malicious code can repurpose the same mathematics for extortion, concealment, covert control, or information theft.

Ransomware is the best-known application, but the field is broader than file encryption. It includes designs in which an attacker keeps a secret advantage—such as a private key—outside the compromised system.

How cryptoviral extortion works

1. The attacker generates an asymmetric key pair and places only the public key or related material in the malware.

2. The malware generates fast symmetric keys on the victim system and encrypts selected data with them.
3. Those symmetric keys are protected with the attacker's public key or otherwise made unavailable to the victim.
4. The corresponding private key remains under attacker control, making correct decryption impractical without it when the implementation has no recoverable flaw.

This hybrid design combines efficient bulk encryption with asymmetric control. Actual ransomware implementations vary, and bugs, reused keys, exposed servers, or recovered key material sometimes allow legitimate decryptors.

Other malicious uses of cryptography

- encrypting configuration, payloads, strings, or command traffic to hinder inspection;
- cryptographically protecting stolen data or staged archives;
- using signatures or keys so malware accepts commands only from its operator;
- concealing stolen information in outputs that look like ordinary cryptographic data;
- creating asymmetric backdoors or kleptographic mechanisms that leak secrets to a key holder.

Terms that are often confused

- **Ransomware** is malware that denies access or threatens disclosure for payment; not every ransomware family uses sound file encryption.
- **Cryptojacking** steals computing resources to mine cryptocurrency. It is not cryptovirology merely because cryptocurrency is involved.
- **Encrypted command traffic** hides content in transit but does not by itself make malware a cryptovirus.

- **Legitimate encryption** can produce high-entropy files and intensive cryptographic activity without being malicious.

Detection ideas

- rapid reads followed by writes, renames, or entropy changes across many user files;
- an unusual process calling cryptographic APIs and traversing local, network, or cloud storage;
- backup deletion, recovery-setting changes, service stops, or security-control tampering before encryption;
- new extensions, ransom notes, inaccessible files, or the same operation across multiple hosts;
- encrypted archives or outbound traffic following bulk collection of sensitive data.

Cryptographic API use and high entropy are not proof. Browsers, backup tools, document systems, VPNs, and security software use encryption legitimately. Correlate process identity, signer, path, data scope, rate, parent process, user, and destination.

Response to malicious encryption

1. Isolate affected systems and shared storage quickly while preserving volatile and endpoint evidence.
2. Do not delete encrypted files, ransom notes, samples, or logs; preserve copies and hashes.
3. Identify the family and incident scope through trusted responders and reputable decryptor resources. Avoid unknown “recovery” executables.
4. Search for initial access, persistence, credential theft, lateral movement, staging, and exfiltration—not only encryption.
5. Rebuild untrusted systems and restore from verified offline or immutable backups after closing the entry path.

Prevention

- maintain isolated, immutable or offline backups and practice full restoration;
- use least privilege, network segmentation, application control, and protected endpoint telemetry;
- patch exposed systems, secure remote access, and use phishing-resistant MFA;
- alert on mass file changes, backup tampering, remote administration, and unusual archive or cryptographic behavior;
- protect key-management and backup administrator accounts separately.

Historical foundation: Young and Yung, Cryptovirology.

Cryptovirology FAQ

Can defenders brute-force ransomware encryption?

Usually not when modern cryptography and key handling are implemented correctly. Recovery depends on backups, implementation flaws, or legitimately recovered keys.

Does paying guarantee recovery?

No. A key may fail, data may be damaged, and stolen data may still be disclosed. Follow legal, incident-response, and law-enforcement guidance.

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