Ransomware response

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: IT leads and management at organizations of any size.

What to do when an attacker encrypts files or systems and demands payment. The goal is to stop the spread, preserve the evidence and restore operations from trusted backups.

Signs it is happening

- Files that will not open and have a new extension.
- A ransom note on the desktop or in the affected folders.
- Backups, shadow copies or antivirus disabled with no explanation.
- High disk and CPU usage on several computers at the same time.
- New administrator accounts or logins at unusual hours.

How serious it is

Critical	Servers, backups or several sites affected; service to the public is down.
High	Several computers in one area encrypted; operations continue in part.
Medium	A single computer affected and isolated, with no signs of spread.

First hour

- [ ] **1.** Disconnect the affected computers from the network: cable and Wi-Fi. Do not power them off.
- [ ] **2.** Disconnect the backups from the network immediately, including external drives and synced cloud storage.
- [ ] **3.** Disable the accounts the attacker may have used, starting with administrator accounts.
- [ ] **4.** Notify management and appoint one single person to coordinate the response.
- [ ] **5.** Take photos of the ransom note and write down the time, computer and user for each finding.
- [ ] **6.** Do not contact the attacker or pay before getting technical and legal advice.

Preparation (before the incident)

- Keep backups under the 3-2-1 rule: three copies, two media, one offline.
- Test restoring at least every quarter; a backup that has never been restored does not count.
- Turn on two-step verification for remote access, email and administrator accounts.
- Do not expose RDP or admin panels to the internet; use a VPN.
- Keep a printed list of emergency contacts: IT, vendor, legal, insurer.

Detection and Analysis

- Identify the ransomware family from the note and the file extension.
- Determine the scope: which computers, which servers, which shared resources.
- Look for the point of entry: email, exposed RDP, unpatched VPN or stolen credentials.
- Check whether data was stolen before the encryption (large outbound traffic, compression tools).

Containment

- Segment the network to isolate the affected areas from the healthy ones.
- Block the identified command-and-control addresses and domains at the firewall.
- Change the passwords of all privileged accounts from a clean computer.
- Suspend scheduled tasks and remote access until you understand the scope.

Eradication

- Reinstall the compromised computers from scratch; do not trust a partial cleanup.
- Fix the vulnerability or the access the attacker used before reconnecting anything.
- Remove any accounts, tasks and tools the attacker left behind.
- Search the rest of the network for the indicators of the attack.

Recovery

- Verify that the backup predates the intrusion and is free of malware.
- Restore the systems critical to operations first, on an isolated network.
- Reconnect in stages and monitor closely for at least two weeks.
- Check nomoreransom.org in case a free decryptor exists for that family.

Lessons Learned

- Bring the team together within the following 15 days and document the timeline.
- Record what worked, what failed and which controls would have prevented the incident.
- Update this playbook and assign an owner and a date to each improvement.

Evidence to preserve

- The ransom note and a sample encrypted file.
- Firewall, VPN, domain controller and antivirus logs.
- A memory image and a disk image of at least one affected computer, if you have the capacity.
- A timeline with date, time, action and person responsible.

What not to do

- Powering off the computers: the evidence in memory is lost.
- Paying the ransom without advice: it does not guarantee recovery and may have legal implications.
- Restoring backups onto computers that have not been reinstalled.
- Connecting backups to the network before the attack is contained.

Who to notify

- Management and legal counsel, from the first hour.
- Staff: what happened, what they must not do and who to report to.
- Customers and affected individuals, if their data was exposed.
- The Public Ministry (Ministerio Público), by filing a criminal complaint with the evidence gathered.
- Your sector's regulator, if applicable (for example, the SIB for supervised entities).
- cert.gt, for guidance and to alert other organizations.

When to close the incident

- Critical systems are operating normally, with no indicators of the attack.
- The point of entry has been identified and fixed.
- All privileged credentials have been changed.
- The incident report has been delivered to management.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

General good-practice guidance; it does not replace legal or specialized technical advice for your case. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).