Malware incident playbook

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

When to use this playbook

Use this playbook when endpoint protection or a user reports malicious software on one or more devices. It excludes extortion cases, which are covered elsewhere.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- Endpoint detection and response or antivirus alerts reach a monitored place.
- Offline, tested backups exist for important data.
- Responders can isolate a device remotely.
- A clean rebuild image exists for each standard device.

Workflow

Work in this order. Record each step and its time in the incident log.

1. Validate the alert and identify the device, user and malware family if known.
2. Short-term containment: isolate the device from the network. Do not power it off if memory evidence may be needed.
3. Check for spread: other devices with the same file, shared drives, and accounts used on the device.
4. Reset passwords and revoke sessions for any account that was used on the infected device.
5. Take a backup image of the affected system before wiping it.
6. Eradicate: reimage from a trusted source, replace compromised files with clean versions, and patch what was exploited.
7. Recover: restore data from a verified backup onto the clean system, and watch it for signs of re-infection.

Decision points

Stop at each of these and record the decision, the decider and the time.

Decision	Who decides	Information needed
Is this a single device or a spread?	Technical lead	Alerts, file hashes, network connections
Rebuild or clean in place?	Technical lead	Malware type, risk of rootkits, time to rebuild
Is data stolen?	Technical lead, privacy lead	Outbound traffic, staging files, cloud sync

Notices to check

Open section 10 of the plan and confirm whether any of these start a notice clock.

- If data left the network, assess it under the data breach plan.
- If the malware reached systems that run a service for customers, check customer contract notice terms.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- Malware removed from every device or the device rebuilt.
- Credentials reset.
- No new alerts for [period].
- The infection route is found and closed.