



Shamoon: How this destructive wiper disables systems

What it is Shamoon, also known as DistTrack, is destructive malware designed to erase data and make Windows computers unusable. It became widely known after attacks against organizations in the Middle East. Later waves reused or changed...

PUBLISHER

Gridinsoft Support

UPDATED

Jul 17, 2026

READ TIME

1 min

What it is

Shamoon, also known as DistTrack, is destructive malware designed to erase data and make Windows computers unusable. It became widely known after attacks against organizations in the Middle East. Later waves reused or changed components, but the central purpose remained disruption rather than recoverable encryption for payment.

How it works

Attackers first obtain privileged access to the target environment. A propagation component can copy the malware to other systems, while a wiper overwrites files and disk structures, sometimes using an embedded driver for low-level access. A reporting component can send execution details

back to the operator before systems fail.

Key points

- Large-scale simultaneous wiping usually means the attackers compromised administrative credentials or deployment paths earlier.
- Standard file recovery may be impossible after disk sectors and file contents are overwritten.
- The visible wiper is the final stage, so investigation must look for the original intrusion and lateral movement.

What to do

- Protect offline backups and clean identity infrastructure before reconnecting recovery systems.
- Isolate affected segments while preserving safe business and industrial operations.
- Rebuild endpoints from trusted media and rotate privileged credentials.
- Test destructive-attack recovery plans, including operation without normal directory and management services.

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](https://support.gridinsoft.com)