S

# Shamoon (Disttrack): Destructive Wiper Behavior and Recovery

Shamoon, also called Disttrack, is destructive malware designed to erase data and disable Windows systems. Learn its behavior, response priorities, and recovery lessons.

PUBLISHER
Gridinsoft Support

UPDATED
Sep 1, 2026

READ TIME
4 min

CONTENTS

## In this guide

**Quick answer:** Shamoon, also known as Disttrack, is destructive Windows malware used in targeted campaigns to overwrite files and disk structures across many computers. Its goal is disruption, not recoverable encryption. If a Shamoon-like outbreak is suspected, isolate network segments, protect identity and management systems, preserve representative evidence, and prepare to rebuild affected endpoints from trusted media.

## 01 What is Shamoon?

Shamoon became widely known after destructive attacks in 2012 and returned in later waves, including campaigns reported in 2016 and 2018. Public research has focused on organizations in the Middle East, particularly energy and government-related targets. The malware family is commonly divided into components for installation, communication, and wiping, although implementations changed between campaigns.

“Shamoon” and “Disttrack” are analytical labels. A damaged Windows fleet should not be attributed from one filename, image, or old IP address. Confirm the sample, timeline, delivery path, credentials, and behavior.

## 02 How the destructive stage works

Reported variants enumerate files and overwrite their contents, then damage boot-related disk structures so systems cannot start normally. Some versions use an embedded driver to access disks. A scheduled activation time can make many compromised hosts fail together, turning a security incident into an immediate business-continuity crisis.

The malware may display or write a selected image while destroying data, but visual artifacts vary and can be copied. The operational signal is coordinated high-volume overwriting and boot failure.

## 03 How attackers reach many devices

Shamoon’s destructive payload is normally the final stage of a broader intrusion. Attackers need a way into the environment and sufficient privileges to distribute or execute it. Stolen administrative credentials, writable network shares, remote administration, scripts, and existing management infrastructure can enable scale. The exact access path differs by incident.

Patching one vulnerability is therefore not a complete Shamoon defense. Identity tiering, segmentation, endpoint controls, and protected software distribution are essential.

## 04 Warning signs

- the same unusual executable, service, task, or script appears on many Windows hosts;
- administrative accounts access large groups of endpoints outside normal maintenance;
- processes open and overwrite many unrelated files or write directly to disks;
- security, backup, or management controls are disabled before a common activation time;
- many systems reboot or fail to boot within a short period;
- network shares, deployment systems, or domain infrastructure show unexpected privileged activity.

## 05 Immediate response

1. **Activate incident and continuity plans.** Coordinate security, infrastructure, operations, safety, legal, and leadership teams.
2. **Segment quickly.** Isolate affected hosts and restrict administrative protocols, shares, and east-west movement while preserving essential operations.
3. **Secure identities.** Disable confirmed compromised accounts and rotate privileged and service credentials from clean administration systems.
4. **Protect management planes and backups.** Review domain, endpoint management, virtualization, software deployment, and recovery consoles for attacker access.

5. **Preserve representative evidence.** Capture memory where feasible, disk images, samples, logs, deployment records, and network telemetry before rebuilding every host.
6. **Find the activation mechanism.** Hunt for scheduled tasks, services, scripts, policies, and remote execution that could trigger remaining systems.

## 06 Recovery

Do not expect a decryptor to restore overwritten data. Reimage affected devices from trusted installation media and known-good configurations. Restore clean data by business priority in a segmented recovery environment. Validate identity, DNS, management, security, and backup services before reconnecting application systems.

Reset secrets in a controlled sequence so new credentials are not exposed to compromised hosts. Reconnect by waves and monitor for the original access path, renewed privileged execution, and destructive file activity. A disk that appears repairable may still contain modified boot code or attacker persistence.

## 07 Preparation and prevention

Separate privileged administration from email and browsing, use secured admin workstations, and restrict service-account logon. Segment user endpoints, servers, management, and backups. Application allow-listing and endpoint behavioral controls can restrict unknown drivers, mass file modification, and remote execution.

Maintain offline or immutable backups under separate credentials and test bare-metal rebuilding, not only file restoration. Keep golden images, installation media, network configurations, identity recovery procedures, and offline contact lists. Conduct exercises where hundreds of endpoints and normal management tools are unavailable simultaneously.

## 08 Frequently asked questions

### Is Shamoon ransomware?

No. Shamoon is a destructive wiper. It overwrites data and system structures rather than maintaining a reliable payment-based recovery path.

### Can antivirus remove it after activation?

Detection may stop remaining payloads, but overwritten files and damaged systems require reconstruction and restoration from clean sources.

### Are old Shamoon indicators still useful?

They support historical hunting, but current defense must emphasize behavior, privileged distribution, identity compromise, and destructive disk access.

**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**