K

Kovter Malware: Fileless Persistence, Detection, and Removal

Kovter is a historic Windows click-fraud malware family known for keeping much of its malicious code in the registry and executing through trusted components.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is Kovter?
02 How the persistence worked
03 Possible signs
04 Detection and investigation
05 How to respond
06 Prevention
07 Sources

Quick answer: Kovter is a historic Windows malware family best known for click fraud and registry-based, nearly fileless persistence. Microsoft documented variants that stored most malicious code in the registry and used a custom file association to launch it through legitimate Windows components. A detection requires more than deleting one downloaded file.

01 What is Kovter?

Kovter evolved across multiple campaigns. Public analysis described click-fraud behavior that generated artificial advertising traffic and earned money for operators. Its persistence techniques made it notable as an example of “fileless” malware, although Microsoft carefully described a later version as almost fileless rather than literally having no file-related artifacts.

Kovter is a family name, so filenames, registry paths, certificates, delivery methods, and network infrastructure can differ. Much public technical reporting is historical. A current alert may represent an old sample, reused technique, archived attachment, or active infection; validate execution and telemetry rather than assuming a decade-old campaign remains unchanged.

02 How the persistence worked

Microsoft documented Kovter creating a shell-open command for a randomly chosen file extension. A corresponding file caused Windows to invoke a legitimate program and execute code stored largely in registry values. This indirect chain made the registry central to persistence and reduced the usefulness of searching only for a conventional malware executable.

Fileless does not mean invisible, harmless, or impossible to remove. Execution still produces behavioral evidence such as process creation, registry modification, scripting or command activity, and network communication. Memory and registry telemetry become more important than a simple disk scan.

03 Possible signs

- An antivirus or EDR verdict naming Kovter or suspicious file-association persistence.
- Unexpected shell-open handlers, encoded registry data, or autorun changes.
- Legitimate Windows processes started with unusual command lines or parent processes.
- Advertising or browsing traffic inconsistent with user activity.
- Repeated detections after a file is removed because the persistence chain remains.

These signs are not exclusive to Kovter. Export the exact registry locations and process tree before cleanup when incident investigation is required.

04 Detection and investigation

Record the security-product verdict, timestamp, user, initial file or email, process ancestry, command line, registry keys, network destinations, and any secondary payload. Review script engines, scheduled tasks, WMI, services, and startup locations for related persistence. Enterprise defenders should search across endpoints for the same delivery attachment, hash, registry pattern, and behavior.

Do not paste old registry-deletion commands from an unrelated sample into a production computer. Removing the wrong file association or registry key can damage Windows or destroy evidence.

05 How to respond

1. Disconnect the device from networks to stop fraudulent traffic and command communication.
2. Preserve alerts and volatile evidence when required. Identify whether code executed and which user context was involved.
3. Update the trusted security product and run a full and offline scan capable of inspecting registry and memory persistence.

4. Investigate the delivery path and other payloads. Secure accounts if credential access or additional infostealers are found.
5. Reimage important or managed systems if the persistence chain cannot be confidently removed and verified.

06 Prevention

Keep Windows, browsers, and document software supported and patched. Block macros from internet-originated documents and restrict risky script interpreters where business use permits. Use least privilege, application control, endpoint behavioral monitoring, email filtering, and centralized registry and process telemetry. Preserve tested backups and a clean deployment method.

07 Sources

Microsoft explains Kovter's registry persistence in its fileless-threat guidance and Kovter technical analysis.

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