



Poweliks: How this fileless Trojan hides in the Windows Registry

What it is Poweliks is a Windows Trojan known for fileless or low-file persistence techniques. Instead of relying on an obvious executable stored on disk, variants place encoded malicious code in the Windows Registry and use legitimate...

PUBLISHER

Gridinsoft Support

UPDATED

Jul 17, 2026

READ TIME

2 min

What it is

Poweliks is a Windows Trojan known for fileless or low-file persistence techniques. Instead of relying on an obvious executable stored on disk, variants place encoded malicious code in the Windows Registry and use legitimate system components to execute it. Poweliks can act as a downloader and may introduce click-fraud, advertising, or other payloads.

How it works

Initial access has included exploit kits, malicious documents, and drive-by downloads. Registry entries launch script or command components through trusted Windows processes, which makes a simple search for a suspicious program file insufficient. The malware contacts remote

infrastructure and can consume resources while performing advertising fraud or fetching more code.

Key points

- Fileless describes where important code runs or persists; it does not mean there are no artifacts to investigate.
- Unusual use of scripting engines and system utilities can be more revealing than filenames.
- Deleting one Registry value without stopping active components may lead to failed or incomplete cleanup.

What to do

- Disconnect the endpoint and collect process, Registry, scheduled-task, and network evidence.
- Use a security tool that examines memory and persistence, not only files on disk.
- Patch the browser, document software, and operating system that allowed initial execution.
- Reimage the device if additional payloads or the full persistence chain cannot be excluded.

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)