P

Poweliks Malware: Registry Persistence, Detection, and Safe Removal

Poweliks is a registry-resident Windows Trojan often called fileless malware. Learn how it persists, what evidence matters, and how to remove it without risky Registry edits.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 How Poweliks works

02 Why "fileless" does not mean invisible

03 Signs worth investigating

04 Safe response and removal

05 What to do about a possible false positive

06 Prevention and monitoring

07 Frequently asked questions

08 References

Poweliks is a Windows Trojan that became known in 2014 for storing its persistent malicious code in the Windows Registry and executing it through memory and legitimate system tools. Later variants were used for click fraud, system profiling, command-and-control, and downloading additional malware.

Poweliks is often called "fileless," but that does not mean an infection leaves no evidence. The initial delivery may involve a file or exploit, Windows stores Registry data on disk, and execution creates observable processes, memory, registry, and network artifacts.

01 How Poweliks works

Public analysis of registry-resident variants describes a multi-stage chain:

1. An installer or exploit gains code execution and writes encoded malicious data into Registry values.
2. A startup entry causes a legitimate Windows program such as `rundll32.exe` to execute JavaScript that reads the next stage from the Registry.
3. Additional script and memory stages can use PowerShell and launch or inject code into legitimate processes.
4. A watchdog mechanism checks whether the malware is running and can restore persistence that defenders remove incompletely.
5. The payload contacts command-and-control infrastructure for click-fraud activity, instructions, or additional malware.

Some variants used non-printable characters and modified permissions to make malicious Registry entries difficult to view or delete with the standard Registry Editor.

02 Why "fileless" does not mean invisible

Common assumption	More accurate explanation

No malicious EXE on disk means nothing can detect it.	EDR and antivirus can inspect Registry writes, script content, process behavior, memory, AMSI events, and network activity.
All use of rundll32 or PowerShell is malicious.	Both are legitimate tools. The command line, parent process, content source, destination, and related activity determine risk.
Deleting one visible key removes Poweliks.	Protected keys, a watchdog process, memory-resident stages, or a separate initial-access component can recreate persistence.
A "Poweliks" label always identifies the original family.	Some products use generic or heuristic labels for similar registry or exploit artifacts. Validate the exact object and behavior.

03 Signs worth investigating

- A security product reports Poweliks or a related registry-resident detection and identifies a Registry value, process, or memory object.
- `rundll32.exe` executes JavaScript or script content sourced from the Registry in a way that is not part of approved software.
- Obfuscated JavaScript or PowerShell launches from an autorun location and creates unusual child processes.
- Unexpected `dllhost.exe` or browser-related processes show injected, network-active code.
- Registry keys are unreadable, have unusual value names, or reappear after deletion.
- A device produces abnormal advertising or click traffic, repeated outbound connections, high process activity, or secondary malware alerts.

None of these clues alone proves Poweliks. Capture the full alert, Registry path and value, process tree, command line, file hashes, memory findings, and network destinations.

04 Safe response and removal

1. **Disconnect the device from networks.** This stops click-fraud traffic, command retrieval, and possible secondary downloads.

2. **Preserve the detection details.** Export the security-product report and collect endpoint telemetry before rebooting or manually changing the Registry.
3. **Run an updated, vendor-supported scan.** Use a security product capable of behavioral, memory, script, and Registry inspection. An offline or recovery-environment scan can help when active processes protect persistence.
4. **Let the security tool remove the complete chain.** Do not paste Registry-deletion commands from an old guide; variants and legitimate software can use nearby locations, and malformed changes can damage Windows or user profiles.
5. **Scan again after restart.** Confirm that persistence and active memory stages do not return.
6. **Look for the entry vector and secondary payloads.** Patch Windows and applications, inspect browser and email history where appropriate, and review other alerts and downloads.
7. **Protect accounts.** If browsers, email, financial accounts, or credentials were used while the host was compromised, change passwords from a clean device, revoke sessions, and enable MFA.
8. **Rebuild when confidence is low.** For a business system, repeated detection, unknown secondary payloads, or evidence of broader compromise can make a trusted reimage safer than repeated manual cleanup.

05 What to do about a possible false positive

Do not exclude an entire Registry branch or allow all script execution. First update the security product, rescan, and record the exact object. Check whether the key belongs to approved software and whether related processes or network behavior exist. If evidence is inconsistent, submit the alert details or sample through the security vendor's false-positive process. Keep the item quarantined until the vendor or an analyst confirms it is benign.

06 Prevention and monitoring

- Apply Windows, browser, Office, and third-party application updates promptly.

- Block untrusted scripts and active content from email and downloads.
- Use attack-surface reduction, application control, and script logging appropriate to the environment.
- Monitor autorun Registry changes and unusual script execution by `rundll32.exe`, PowerShell, and other trusted Windows binaries.
- Use web and DNS controls to block known malicious infrastructure.
- Keep tested backups and a documented endpoint rebuild process.

07 Frequently asked questions

Is Poweliks a virus?

It is generally classified as a Trojan, not a self-replicating file virus. It relies on delivery and execution mechanisms and can fetch other payloads.

Can I find Poweliks in Task Manager?

You may see abused legitimate processes, but their names alone will not identify the injected code. Use endpoint telemetry or a security scanner that inspects memory, command lines, scripts, and Registry persistence.

Can Poweliks affect macOS or phones?

The documented Poweliks family targets Windows mechanisms. A similar name on another platform should be verified against the vendor's detection description rather than assumed to be the same malware.

08 References

- Symantec/Broadcom: Poweliks click-fraud malware goes fileless
- Microsoft: Fileless threats

- MITRE ATT&CK: Rundll32 (T1218.011)
- F-Secure: Trojan:W32/Poweliks

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