A

Amonetize Adware: What the Detection Means and How to Remove It

Adware.Amonetize is a generic detection for Windows bundlers that combine a desired program with advertising or pay-per-install offers. Learn how to remove the bundle and related PUPs.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 How to interpret an Amonetize detection
02 How Amonetize bundlers reach a PC
03 Possible signs that bundled adware ran
04 How to remove Amonetize and related components
05 Why the alert keeps returning
06 Is Amonetize dangerous?
07 Could it be a false positive?
08 How to avoid software bundles
09 Frequently asked questions
10 Reference

Adware.Amonetize is a generic detection name associated with Windows software bundlers that combine a desired program with advertising components or pay-per-install offers. The alert may identify the original installer, an extracted component, or an additional application delivered by the bundle.

Amonetize is not one fixed virus with one hash or behavior. Security products may classify related files as adware, PUP, PUA, bundler, or download manager. Keep the detection quarantined and use its exact path and execution history to determine whether the package merely downloaded or actually installed other software.

01 How to interpret an Amonetize detection

Detection location	Likely situation	Recommended action
Downloads or unopened archive	The bundler may not have executed	Quarantine and delete the complete package
Browser cache or temporary folder	A download or advertising artifact was stored	Close the browser, clear the relevant site data, and rescan
Temp or AppData after setup ran	The installer extracted or launched components	Review newly installed applications and browser changes
Program Files, startup, or extension path	A bundled component may be installed	Uninstall it, remove persistence, and run a full scan
Same alert repeatedly returns	An installer, updater, sync source, or browser is recreating it	Identify and remove the source rather than only the copy

02 How Amonetize bundlers reach a PC

- General-purpose download portals that wrap an original program in their own installer.
- Search advertisements and fake download buttons.
- Free utilities, converters, media tools, game modifications, cracks, or repacked installers.

- Deceptive update notices or redirect chains.
- Optional offers presented through confusing, preselected, or rushed installation screens.

A desired application can work as promised while the surrounding bundle remains unwanted. Successful installation does not prove that the wrapper or every additional offer is safe.

03 Possible signs that bundled adware ran

- New advertising appears across unrelated websites or outside the browser.
- The home page, search engine, new-tab page, proxy, or notification permissions changed.
- Unknown extensions, shopping helpers, optimizers, trials, or download managers appeared.
- Pop-ups and redirects return after the original installer closes.
- Several PUP or adware detections share the same installation time.
- A background process or startup entry recreates the detected file.

Advertising on one website alone may come from that site's normal ad system. If the behavior follows one browser across many sites, inspect the browser and device.

04 How to remove Amonetize and related components

1. **Keep all detections quarantined.** Record their names, full paths, hashes, and timestamps.
2. **Delete the source installer.** Remove archives, extracted folders, disk images, and duplicates from Downloads, email, cloud sync, and Recycle Bin.
3. **Review software by installation date.** Uninstall unknown or unwanted applications added during the same session. On a work device, ask IT before removing managed software.
4. **Inspect browsers.** Remove unwanted extensions and notification permissions and restore intended search, startup, home-page, proxy, and DNS settings.

5. **Review persistence.** Check startup apps, scheduled tasks, services, and background items associated with the bundle.
6. **Update and scan.** Run a full scan with current security intelligence and review every additional detection independently.
7. **Restart and verify.** Confirm that ads, redirects, applications, and detections do not return.

05 Why the alert keeps returning

The source may remain in a synchronized folder, browser cache, email attachment, backup, or installer that runs at startup. Compare paths and hashes across alerts. If the exact file changes, capture the process that creates it. Do not exclude Downloads, Temp, AppData, or the browser cache, because broad exclusions create a durable hiding place for future threats.

06 Is Amonetize dangerous?

The risk ranges from an unwanted installer wrapper to a chain that introduces more intrusive software. Adware can track browsing, inject advertising, redirect traffic, change settings, and weaken user control. The same download source may also distribute unrelated malware. If a stealer, RAT, miner, or Trojan was detected, treat it as a separate compromise rather than assuming it is harmless adware.

07 Could it be a false positive?

A file can be functional yet accurately classified as a PUA because of bundling, consent, advertising, or pay-per-install behavior. For authorized business software, verify the exact hash, digital signature, publisher, source, installation behavior, and vendor analysis. Submit the sample to the detecting vendor before creating a narrow, temporary exception.

08 How to avoid software bundles

- Download from the original publisher, an operating-system store, or an approved catalog.

- Avoid search advertisements, mirrors, cracks, and generic download buttons.
- Read every installer screen and decline optional applications, extensions, and notification permissions.
- Enable potentially unwanted app blocking and reputation-based protection.
- Use standard user accounts and application control on managed endpoints.

09 Frequently asked questions

Is Adware.Amonetize a Trojan?

It is primarily a generic adware or bundler detection. A package can deliver separate Trojans, so review all alert names and behavior.

Does deleting the installer remove everything?

Only if it never ran. If setup executed, inspect installed applications, browser changes, persistence, and additional detections.

Should I restore the file?

No for ordinary use. Obtain the desired application directly from its official publisher without the third-party wrapper.

10 Reference

- Malwarebytes Threat Center: Adware.Amonetize

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