

Heimdal data reveals MediaArena adware completes persistence before antivirus quarantine finishes

Heimdal's Threat Intelligence team directly measured, using its own telemetry, the timeline of a real infection.

LONDON, UNITED KINGDOM, July 30, 2026 /EINPresswire.com/ -- New data from [Heimdal](#)'s telemetry measures the gap between execution of the MediaArena adware and the completion of quarantine. The same pattern has been confirmed across more than 40 client environments.

MediaArena is a browser-modifier adware family that Microsoft has tracked since 2023. It is low-severity, and that is what makes the finding notable. Even a nuisance-grade detection can finish establishing persistence before antivirus intervenes. The malvertising cluster spreading it has been publicly documented since March and was analysed by Compass Apex Security in April. It reaches victims through fake "free AI tool" ads.

Using its own telemetry from live client environments, Heimdal measured the timeline of a MediaArena infection. The adware finished writing its persistence mechanism to disk 21 seconds after execution. Microsoft Defender's quarantine did not finish until 29 seconds, a full eight seconds after the infection had already taken hold.

This measurement comes from direct observation of Heimdal's own customer base, not from a lab or a sandbox.

The pattern is not an isolated case. Heimdal has observed the same sequence, persistence completing before quarantine finishes, across more than 40 client environments in recent days. In the case Heimdal timed, signature-based detection then took roughly 78 days to catch up, leaving the browser hijacker running for around eleven weeks.



New Heimdal telemetry measures the gap between MediaArena's execution and antivirus quarantine - a pattern confirmed across 40+ client environments.

"We timed a MediaArena infection and the persistence was on disk before the quarantine even finished. The alert isn't wrong, it's just late. By the time it fires, the adware has already done what it came to do, so a team that stops at 'quarantined' is working from an incomplete picture," said Alexandru Gurgu, Threat Intelligence Security Analyst at Heimdal.

The takeaway for security teams is direct. A quarantine alert is not proof that an endpoint is clean. For MediaArena, the alert may simply mark the moment detection caught up, not the moment the threat was stopped.

Heimdal recommends treating a MediaArena quarantine alert as the start of an investigation, not its conclusion, and checking affected endpoints directly for persistence artefacts.

Read the full report here: <https://heimdalsecurity.com/blog/media-arena-malvertising-report/>

About Heimdal

Heimdal is a global cybersecurity provider offering a [unified security and compliance platform](#) across endpoint, identity, email, network, and access security. More than 17,000 customers and 1,500 MSPs in over 40 countries use its 12-plus integrated products to prevent threats, detect breaches, and automate response.

Danny Mitchell
Heimdal Security
+44 7999 498241

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/930454180>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.