AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-15 20:40:17 (EDT - America/New_York) | 2026-07-16 00:40:17 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 765 bytes
IOCs Found: 2
ATT&CK Techniques: 0

Severity

Low

Confidence

10% - Very Low Confidence

Confidence Factors

None

Reducing Factors

• Valid digital signature from Electronic Arts, Inc.
• No malicious or suspicious detections from 71 antivirus engines on VirusTotal
• No packers detected
• MalwareBazaar reports no matches for the file hashes

Threat Type

Insufficient Evidence

Executive Summary

The file EAappInstaller.exe is a signed Windows executable from Electronic Arts, Inc. with no detections on VirusTotal and no matches in MalwareBazaar. The file entropy is moderately high but no suspicious behavior or threat intelligence is observed.

Evidence Supporting Assessment

• File is signed by Electronic Arts, Inc. with a valid signature dated 09/19/2023
• VirusTotal shows 0 malicious or suspicious detections out of 71 engines
• MalwareBazaar reports no known malware matches for the SHA1 and SHA256 hashes
• PE section entropy values are within normal ranges for legitimate executables
• No packers or obfuscation detected in the file metadata

Ambiguity Notes

• No behavioral telemetry or runtime analysis data is available to confirm benign or malicious behavior
• High entropy could indicate packing or compression but no packer was detected
• Absence of detections does not guarantee the file is free from risk
• No information about the file's origin or distribution context is provided

Alternative Hypotheses

• Legitimate installer executable for Electronic Arts software
• Potentially a new or custom installer not yet detected by antivirus engines
• Benign file used in a controlled environment or testing

Alternative Explanations

• File is a legitimate software installer signed by a trusted publisher
• File is a benign update or patch component for Electronic Arts software

Indicators of Compromise

Hashes
- d024f8dab352a5f738534167237adb6d779afe40
- faa5a84578ac440db65439d936192c6baef20419b66652275704591aa9861183

MITRE ATT&CK Mapping

None

Recommended Actions

- Verify the file source and distribution channel to confirm legitimacy
- Confirm the digital signature details and publisher reputation
- Monitor for any unusual behavior if the file is executed in the environment

Analyst Notes

None

AI-Assisted Analysis Disclaimer

This report was generated using AI-assisted analysis and is intended to support security investigations. Findings, conclusions, and recommendations should be reviewed and validated by a qualified analyst before operational, legal, or business decisions are made.