# Malware Analysis Report**: W32.HfsAdware.5066**

## Inter id:246

## 1.Basic Identification

Malware Name: W32.HfsAdware.5066

Type: Adware

Platform: Windows (32-bit)

SHA256 Hash: 27c6adc401e509a9e76633df6d3ccb3e91b3d60ed1cb65d522f32efc9e97f238

## 2.Checklist-Based Static Analysis Summary

- File Type & Size: Likely a `.exe` binary (PE32)

- Hash Validation: SHA256 matched

- Strings Analysis: Ad-related URLs, registry keys, or system calls

- PE Structure Check: Typical adware imports (Wininet.dll, Shell32.dll, etc.)

- Obfuscation/Packing Detected: Possibly packed (e.g., UPX)

- Suspicious APIs: CreateProcess, RegSetValue, ShellExecute, etc.

- Auto-Startup Persistence: Likely via Windows Run registry keys

- Network Indicators: Connects to ad servers

- Ad Behavior: Browser redirects, ad popups

## 3.Dynamic Behavior (Expected)

**-**Drops files in %AppData% or %Temp%

- HTTP communication with ad/tracker domains

- Modifies registry for persistence

- Drops helper .dll/.exe files

- No known Command and Control server interaction

## 4.Threat Level: Low to Moderate

-This adware is not directly destructive but can degrade system performance, expose users to ads and potential secondary threats.

## 5.Recommended Mitigation

-Use a reputable antivirus to remove

-Manually remove autorun entries and dropped files

-Quarantine by hash

- Block contacted domains

- Use System Restore if needed

## 6.Additional Notes

-No signs of rootkit behavior

- Likely bundled with freeware

- User education recommended

## 5.Recommended Mitigation

-Use a reputable antivirus to remove

## 5.Recommended Mitigation

-Use a reputable antivirus to remove

Manually remove autorun entries and dropped files

- Quarantine by hash

- Block contacted domains

- Use System Restore if needed

## 2.Additional Notes

- No signs of rootkit behavior

- Likely bundled with freeware

- User education recommended

Manually remove autorun entries and dropped files

- Quarantine by hash

- Block contacted domains

- Use System Restore if needed

## 3. Additional Notes

- No signs of rootkit behavior

- Likely bundled with freeware

- User education recommended