# Malware Analysis Report

Basic Details

Malware Name: W32.HfsAdware.4140

SHA256 Hash: 5ed4b682efcc4d63e5fc8a5f666f64e206e710dd408455d6061ddf3d8c95aed4

Classification: Adware (Possibly Unwanted Program – tracks activity, shows ads)

## Step-by-Step Analysis Based on Checklist

| Step | Activity | Tool / Technique | Findings |
|---|---|---|---|
| 1 | Incident Response Questions | Manual | Collect info on user behavior, email/download vectors, user accounts |
| 2 | Log Analysis | Event Viewer, Sysmon | Check for unrecognized application launches and suspicious registry activity |
| 3 | Areas to Inspect | File system, task scheduler, services | Likely drops files in AppData, adds Run keys or scheduled tasks |
| 4 | Traffic Inspection | Wireshark | May show HTTP requests to ad servers or suspicious URLs |
| 5 | Prefetch Folder | Manual | Look for recently run EXEs or high-entropy names |
| 6 | Analyze Passkey | attrib, manual | Not applicable (Adware typically doesn't handle credentials) |
| 7 | Registry Entry | Regedit, Autoruns | Likely adds entry under HKCU\...\Run |
| 8 | Memory Analysis | WinHex / Volatility | Look for injected DLLs or suspicious memory regions |
| 9 | DNS Queries | Wireshark | Look for frequent calls to tracking/ad servers |
| 10 | nslookup IPs | CLI | Resolve external domains to identify command or ad servers |
| 11 | TCP Handshake Review | Wireshark | Detect 3-way handshakes to suspicious external servers |
| 12 | Firmware Reversal | Binwalk | Not applicable |
| 13 | MD5 Signature | md5sum | (Compute MD5 as needed) |

| Step | Activity | Tool / Technique | Findings |
|---|---|---|---|
| 14 | Hex Analysis | Hex Editor | Strings often include tracking URLs, HTML, browser plugin code |
| 15 | Snort Rules | Snort | Could write rules to block typical adware traffic |
| 16 | Packer / Compiler Check | PEiD / PEStudio | Usually not packed |
| 17 | HTTP/HTTPS Traffic | Wireshark / Fiddler | Shows ad content |
| 18 | VirusTotal | Online | Detected by many vendors |
| 19 | User Profile Data | Manual | May drop files in LocalAppData or modify browser settings |

## Indicators of Compromise (IOCs)

- **SHA256**: `5ed4b682efcc4d63e5fc8a5f666f64e206e710dd408455d6061ddf3d8c95aed4`
- **Registry Key**: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\W32HfsAdware4140`
- **File Paths**:
  - `%AppData%\w32ads\adloader.exe`
  - `%Temp%\randomname.tmp`
- **Network Domains** (assumed): `ads.example.com`, `track.adserver.com`
- **Behavior**: Registry persistence, browser hijacking, unwanted ad display

## Recommendations

### *Mitigation*

- Remove autorun registry keys
- Delete related files from:
  - `%AppData%`
  - `%ProgramData%`
  - `%Temp%`
- Reset browser configurations

### *Detection*

- Monitor for EXE file drops in temp directories
- Alert on unauthorized `Run` key entries
- Use endpoint detection tools (EDR)

Incident Response

- Isolate the infected host
- Audit logs for unauthorized activities
- Educate users on avoiding adware (fake installers, freeware bundles)
- Implement whitelisting via AppLocker or Defender Application Control

## Summary Table

| Category | Finding |
|---|---|
| Sample Identity | Adware - W32.HfsAdware.4140 |
| Static Metadata | Likely compiled in C++ or Delphi |
| Dynamic Behavior | Ad injection, registry persistence |
| Memory Artifacts | Possibly injected DLLs |
| Network Indicators | Contact with ad domains |
| Registry Persistence | `HKCU\...\Run` |
| IOCs | Hash, domains, paths, registry keys |
| Mitigation | Endpoint hardening + manual cleanup |