Malware Analysis Report: W32.HfsAdware.5066

# 1. Basic Details

- Malware Name: W32.HfsAdware.5066  
- Type: Adware  
- SHA256 Hash: 27c6adc401e509a9e76633df6d3ccb3e91b3d60ed1cb65d522f32efc9e97f238

# 2. Checklist-Based Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Activity | Tool/Method Used | Findings / Notes |
| 1 | Incident Response Questionnaire | Manual | Interview team/user for suspicious behavior. Suspicious pop-ups and browser redirects reported. |
| 2 | Log Analysis | Sysmon, Event Viewer | Found unexpected browser launches and registry modifications. |
| 3 | Areas to look for | - | Prefetch, Temp, AppData, Registry, Startup items. |
| 4 | Traffic inspection using Wireshark | Wireshark | Outbound HTTP traffic to ad domains, resolved DNS to suspicious ad networks. |
| 5 | Inspect prefetch folder | Manual | Prefetch file related to ad\_helper.exe found. |
| 6 | Analyze Passkey (Check for file attributes) | attrib command | Hidden executable in AppData\Roaming\adsvc.exe. |
| 7 | Registry Entry for "Run" File | regedit/manual | Entry in HKCU\Software\Microsoft\Windows\CurrentVersion\Run\adsvc. |
| 8 | Memory Analysis | WinHex, Volatility | Memory strings show ad domains, injected into browser processes. |
| 9 | DNS Queries | Wireshark/DNS logs | Frequent queries to domains like adsboost.com, advtrck.com. |
| 10 | Suspicious Process Monitoring | Procmon/Process Hacker | Detected process adsvc.exe auto-starting with obfuscated child processes. |

# 3. Behavioral Summary

|  |  |
| --- | --- |
| Category | Observation |
| File Droppers | adsvc.exe in %AppData%, hidden attributes |
| Registry Mod | Auto-run entry added to Run key |
| Network | HTTP traffic to ad servers |
| Persistence | Registry-based autorun |
| Obfuscation | Base64 encoded strings and obfuscated process name |
| Impact | Slows down browser, serves persistent ads, tracks user activity |

# 4. Indicators of Compromise (IOCs)

|  |  |
| --- | --- |
| Type | IOC |
| File Name | adsvc.exe, ad\_helper.exe |
| Registry | HKCU\...\Run\adsvc |
| Network Domains | adsboost.com, advtrck.com |
| SHA256 Hash | 27c6adc401e509a9e76633df6d3ccb3e91b3d60ed1cb65d522f32efc9e97f238 |

# 5. Remediation Steps

1. Terminate malicious process: taskkill /F /IM adsvc.exe  
2. Remove registry key: reg delete HKCU\...\Run /v adsvc  
3. Delete malicious files from %AppData%  
4. Reset browser settings and extensions  
5. Clean DNS cache: ipconfig /flushdns  
6. Full system AV scan with updated signatures

# 6. Prevention Recommendations

- Block known adware domains at firewall/DNS level  
- Disable autorun from registry via GPO  
- Educate users against clicking on suspicious ads and pop-ups  
- Monitor with endpoint protection and tools like Sysmon + SIEM