Technical Analysis: Adware.WorldWideWeb & WMI Hijacking

1. Executive Summary

This report details the evolution of the **Adware.WorldWideWeb** strain. Previously known for standard persistence methods, recent variants have implemented sophisticated **Windows Management Instrumentation (WMI)** hijacking to actively suppress security software. The **DoesNotBelong** utility successfully neutralized this threat by purging the WMI repository and removing a deep-seated persistence script within the SYSTEM profile.

2. Persistence & Deceptive Signaling

The infection employs a multi-layered approach to ensure its survival and mislead responders:

- **Deceptive Signaling:** Creation of `C:\ProgramData\MalwarebytesRemoval-MbSetupWmi-OK.txt`. This file is a malicious "Status Flag" designed to trick technicians into believing a legitimate cleanup has already occurred.
- **The Engine (SYSTEM Profile):** `C:\Windows\System32\config\systemprofile\AppData\Local\WMILoad\ClockRemoval-WmiBoot.ps1`. This hidden script ensures the WMI repository is re-infected upon system boot.
- **The Watchdog Task:** Deletion of the scheduled task named **"WorldWideWeb"**, which acted as a secondary persistence trigger for the adware's components.

3. Targeted Suppression: WMI Event Filters

The most significant discovery in this variant is the use of high-volume WMI Event Filters specifically targeting the Malwarebytes installation process (`MbSetup`). These filters trigger a "Kill Consumer" the moment security activity is detected.

Verified WMI Remediation Log:

- `[FOUND]: __EventFilter | Name: MbRemovalMbSetupW320 ... [SUCCESS] Removed`
- `[FOUND]: __EventFilter | Name: MbRemovalMbSetupTrace1 ... [SUCCESS] Removed`
- `[FOUND]: __EventFilter | Name: MbRemovalMbSetupW324 ... [SUCCESS] Removed`
- **Active Suppression:** `[FOUND]: CommandLineEventConsumer | Name: MbRemovalMbSetupKillConsumer ... [SUCCESS] Removed`

4. Associated Malicious Directories

The audit identified several randomized directories used to house the adware's primary payloads (e.g., `NetSixUpdater.exe`, `WaveTownEight.exe`):

- `C:\Program Files (x86)\WaveTownEightWorkstation\`
- `C:\Program Files (x86)\GeneralAIFrameworkSolutions\`
- `C:\Program Files (x86)\GeneralAISupport2Solutions\`

5. Remediation via DoesNotBelong

The **DoesNotBelong** utility successfully neutralized **Adware.WorldWideWeb** through the following actions:

1. **WMI Repository Audit:** Identifying and stripping the `MbRemoval` filters and the `KillConsumer` that prevented security remediation.
2. **Task & Script Purge:** Deleting the `WorldWideWeb` scheduled task and the hidden `WMILoad` directory within the SYSTEM profile.
3. **Payload Erasure:** Forcing the removal of randomized `Program Files (x86)` directories and deceptive status flags in `C:\ProgramData`.

6. Conclusion

The transition of **Adware.WorldWideWeb** into WMI hijacking represents a significant escalation in adware behavior. By actively suppressing security tools like Malwarebytes, it moves beyond simple advertising into the realm of aggressive malware. **DoesNotBelong** remains an essential first-response tool for stripping these WMI hooks, allowing standard security suites to resume operation.