# Detection of Adversary-in-the-Middle, Detection Strategy DET0764

Archived: 2026-04-05 16:55:33 UTC

## Analytics

- ICS

### AN1896

Monitor HKLM\Software\Policies\Microsoft\Windows NT\DNSClient for changes to the "EnableMulticast" DWORD value. A value of "0" indicates LLMNR is disabled.
Host-based implementations of this technique may utilize networking-based system calls or network utility commands (e.g., iptables) to locally intercept traffic. Monitor for relevant process creation events.
Monitor for network traffic originating from unknown/unexpected hosts. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware. For added context on adversary procedures and background see Adversary-in-the-Middle and applicable sub-techniques.
Monitor for newly constructed services/daemons through Windows event logs for event IDs 4697 and 7045.
Monitor network traffic for anomalies associated with known AiTM behavior. For Collection activity where transmitted data is not manipulated, anomalies may be present in network management protocols (e.g., ARP, DHCP).
Monitor application logs for changes to settings and other events associated with network protocols and other services commonly abused for AiTM.

#### Log Sources