Detection of Command and Control Over Application Layer Protocols, Detection Strategy DET0444

Archived: 2026-04-05 17:33:42 UTC

AN1225

Detects suspicious usage of common application-layer protocols (e.g., HTTP, HTTPS, DNS, SMB) by abnormal processes, with high outbound byte counts or irregular ports, possibly indicating command and control or data exfiltration.

Log Sources

Mutable Elements

Field	Description
ProtocolList	Limit detection to app-layer protocols of interest: HTTP, DNS, SSL, SMB, RDP
DataVolumeThreshold	Detects asymmetric communication volume (e.g., >90% outbound)
UnusualProcessList	Track processes not normally associated with network activity

AN1226

Detects suspicious curl, wget, or custom socket traffic that leverages DNS, HTTPS, or IRC-style protocols with unbalanced traffic or beacon-like intervals.

Log Sources

Mutable Elements

Field	Description
KnownPortsToMonitor	Uncommon ports for HTTPS, IRC, DNS (e.g., 8443, 5353)
BeaconTimingThreshold	Detect intervals of outbound traffic within fixed timeframes

AN1227

Detects applications using abnormal protocols or high volume traffic not previously associated with the process image, such as Automator or AppleScript invoking curl or python sockets.

Log Sources

Mutable Elements

Field	Description
SocketParentProcessMatch	Non-browser processes opening sockets to external IPs
DataFlowImbalanceRatio	High outbound/inbound ratio indicating C2 beacon

AN1228

Detects application-layer tunneling or unauthorized app protocols like DNS-over-HTTPS, embedded C2 in TLS/HTTP headers, or misused SMB traffic crossing VLANs.

Log Sources

Mutable Elements

Field	Description
AppProtocolAbusePattern	Detects DNS tunneling, encrypted HTTP C2, or malformed headers
NorthSouthEgressFilter	Monitor internal hosts talking externally using internal protocols (e.g., SMB)
