Behavioral Detection of Publish/Subscribe Protocol Misuse for C2, Detection Strategy DET0002

Archived: 2026-04-05 12:43:13 UTC

AN0002

Detects non-standard processes (e.g., PowerShell, python.exe, rundll32.exe) making outbound connections using publish/subscribe protocols (e.g., MQTT, AMQP) over non-browser, encrypted channels, often beaconing to message brokers.

Log Sources

Mutable Elements

Field	Description
UnusualProcessList	Detect suspicious processes initiating outbound pub/sub connections
TimeWindow	Define beaconing interval used for temporal correlation
ProtocolPortList	Custom MQTT/XMPP port use in non-standard ranges (e.g., 1883, 5222, 5672)

AN0003

Detects CLI tools (e.g., mosquitto_pub, nc, python scripts) interacting with pub/sub brokers using unusual topic names, high-frequency publication rates, or obfuscated payloads to non-standard hosts.

Log Sources

Mutable Elements

Field	Description
BrokerAllowList	Known-good brokers used by approved apps and daemons
TopicAnomalyScore	Payload length, entropy, or topic name patterns

AN0004

Detects osascript, curl, or custom binaries interacting with XMPP/MQTT brokers in unapproved destinations with encrypted payloads or frequent POST-like requests to broker URIs.

Log Sources

Mutable Elements

Field	Description
AppContextFilter	Applications not known to use pub/sub protocols
URIPathRegex	Custom path patterns to message brokers over HTTPS

AN0005

Detects pub/sub traffic over unusual ports, high-frequency topic publications, and connections to known-bad or dynamic broker endpoints outside allowlisted infrastructure.

Log Sources

Mutable Elements

Field	Description
BrokerReputationList	Dynamic blocklist or threat intel feed for C2 brokers
PayloadLengthThreshold	Exfil-style long topic messages vs telemetry-style short messages

---