

# Suspicious Use of Web Services for C2, Detection Strategy

## DET0425

Archived: 2026-04-05 16:51:07 UTC

### AN1189

Detects unusual outbound connections to web services from uncommon processes using SSL/TLS, particularly those exhibiting high outbound data volume or persistence.

#### Log Sources

#### Mutable Elements

Field	Description
ProcessName	To tune for unexpected or uncommon executables initiating network connections
DataTransferThreshold	Volume of outbound data in short time window (e.g., >1MB in <5 min)
TimeWindow	Look for connections persisting outside of normal business hours

### AN1190

Detects command-line tools, agents, or scripts making outbound HTTPS connections to popular web services like Discord, Slack, Dropbox, or Graph API in an unusual context.

#### Log Sources

#### Mutable Elements

Field	Description
ParentProcess	Unusual parent-child process behavior initiating external comms (e.g., bash > curl)
HostnamePattern	Destination hostnames (e.g., *.dropboxapi.com, *.graph.microsoft.com)
RequestFrequency	Repeated requests at unusual intervals, suggesting beaconing

### AN1191

Detects user agents or background services making unauthorized or unscheduled web API calls to cloud/web services over HTTPS.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
ProcessSignature	Unsigned or user-modified apps communicating with cloud services
ConnectionInterval	Beacon-like pattern of regular outbound communication

**AN1192**

Detects guest VMs or management agents issuing HTTP(S) traffic to external services without a valid patch management or backup justification.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
RemoteIPRange	Filter to detect only external/public destinations
VMContext	Exclude known backup or patch automation services

---

Source: <https://attack.mitre.org/detectionstrategies/DET0425>