

# Detection Strategy for Exfiltration to Text Storage Sites, Detection Strategy DET0284

Archived: 2026-04-05 16:36:29 UTC

## AN0787

Unexpected processes (e.g., powershell.exe, wscript.exe, office apps) initiating HTTP POST/PUT requests to text storage domains like pastebin.com or hastebin.com, particularly when preceded by file access in sensitive directories. Defender perspective: correlation of process lineage, large clipboard/file read operations, and outbound uploads to text storage services.

### Log Sources

### Mutable Elements

Field	Description
TextStorageDomains	Domains to monitor such as pastebin.com, hastebin.com, ghostbin.com.
UploadSizeThreshold	Minimum data size (e.g., >500KB) to trigger alerts for suspicious uploads.
UserContext	User accounts with legitimate business justification for posting to text storage sites.

## AN0788

Use of curl, wget, or custom scripts to POST data to pastebin-like services. Defender perspective: identify chained behavior where files are compressed/read followed by HTTPS POST requests to text-sharing endpoints.

### Log Sources

### Mutable Elements

Field	Description
AllowedTools	Whitelist of tools (e.g., curl for package repos) to reduce false positives.
WorkHours	Expected time ranges for developer interactions with external paste sites.

## AN0789

Processes such as osascript, curl, or office applications sending data to text storage APIs/domains. Defender perspective: anomalous clipboard or file reads by unexpected applications immediately followed by outbound

HTTPS requests to pastebin-like services.

**Log Sources**

**Mutable Elements**

Field	Description
WatchedApps	Processes not normally associated with data uploads (e.g., Preview, Calculator).
EntropyThreshold	High entropy detection to flag encoded or encrypted data exfiltration.

**AN0790**

ESXi services (vmx, hostd) generating outbound HTTPS POST requests to text storage sites. Defender perspective: anomalous datastore or log reads chained with traffic to pastebin-like destinations.

**Log Sources**

**Mutable Elements**

Field	Description
DatastoreExfilThreshold	Threshold of bytes exfiltrated from ESXi datastore files.
ApprovedDestinations	Whitelist of domains approved for API communication to prevent false positives.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0284>