

# Detection of Exfiltration Over Unencrypted Non-C2 Protocol, Detection Strategy DET0149

Archived: 2026-04-05 18:08:34 UTC

## AN0423

Detects data access or staging events followed by outbound data flows using unencrypted protocols (e.g., FTP, HTTP) initiated by unexpected processes or to rare destinations.

### Log Sources

### Mutable Elements

Field	Description
UnencryptedProtocolList	Set of protocols considered suspicious for outbound data exfiltration (e.g., FTP, HTTP).
DataTransferSizeThreshold	Defines what amount of outbound data is considered abnormal for a host/user.
ParentProcessDenylist	Processes that should not launch FTP/HTTP clients (e.g., winword.exe launching ftp.exe).

## AN0424

Detects file access or compression utilities followed by outbound connections using curl, wget, ftp, or custom binaries communicating over unencrypted protocols.

### Log Sources

### Mutable Elements

Field	Description
SensitiveDirectoryWatchlist	Flag access to paths known to store sensitive or regulated data.
ProcessBaseline	Define which binaries are allowed to communicate externally using HTTP/FTP.
TimeWindow	Correlates process/file/network within a defined time window.

## AN0425

Detects abnormal outbound HTTP/FTP connections by local scripts or binaries outside of standard browser activity, following access to local documents or user data.

**Log Sources**

**Mutable Elements**

Field	Description
ScriptedClientAllowlist	Defines allowed automated agents that may transmit HTTP or FTP data (e.g., backup tools).
PayloadInspectionKeywordList	Terms or patterns indicating structured or sensitive data leaving via HTTP/FTP.

**AN0426**

Detects shell-based scripts accessing configuration files or snapshots and transmitting them over unencrypted protocols such as FTP or HTTP to non-management IPs.

**Log Sources**

**Mutable Elements**

Field	Description
VMConfigAccessPathWatchlist	Locations of VMX/CFG/SNAPSHOT files that should not be accessed by non-admin shells.
OutboundProtocolProfile	Expected network protocols for guest and host interfaces.

**AN0427**

Detects use of unencrypted protocols (e.g., TFTP, FTP, HTTP) to transfer configuration files, routing tables, or logs to untrusted IP addresses, especially using administrative commands like `copy run ftp: .`

**Log Sources**

**Mutable Elements**

Field	Description
ProtocolCommandWatchlist	Flag commands like <code>`copy`</code> , <code>`archive tar`</code> , or <code>`upload`</code> directed at external hosts.
DestinationIPBlocklist	Define external IP ranges unauthorized to receive router/switch configs.

Source: <https://attack.mitre.org/detectionstrategies/DET0149>