Detect Ingress Tool Transfers via Behavioral Chain, Detection Strategy DET0060

Archived: 2026-04-05 17:14:54 UTC

AN0165

Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Tune for known good updaters (e.g., ChromeUpdate, OneDrive)
DestinationIPCategory	Allow filtering by internal vs external IP blocks
FilePathRegex	Focus on uncommon file drop paths (e.g., C:\Users\Public\)

AN0166

Shell-based tools (curl, wget, scp) initiate connections to external domains followed by creation of executable files on disk.

Log Sources

Mutable Elements

Field	Description
ToolName	Match on curl, wget, rsync, etc. based on environment
DownloadExtension	Tunable filter to limit to suspicious file types (.sh, .bin, .elf)

AN0167

Process execution of curl or wget followed by a network connection and a file created in temporary or user-specific directories.

Log Sources

Mutable Elements

Field	Description
DirectoryTargeted	Restrict to high-risk directories like /Users/Shared, /tmp/
ProcessPath	May tune based on custom tooling or MDM activity

AN0168

Command line interface or vCLI triggers remote transfer using wget or curl, writing files into datastore paths or local tmp directories.

Log Sources

Mutable Elements

Field	Description
ToolName	Tune for wget, curl, netcat, and scripting languages in use
DatastorePath	Filter or prioritize specific paths (e.g., /vmfs/volumes/)

AN0169

Network device logs show anomalous inbound file transfers or uncharacteristic flows with high payload volume to network devices with storage or automation hooks.

Log Sources

Mutable Elements

Field	Description
PayloadVolumeThreshold	Tune based on expected update size vs anomalous bulk data transfers
ProtocolUsed	Flag unexpected protocols like TFTP, FTP, HTTP
