Detection of File Transfer Protocol-Based C2 (FTP, FTPS, SMB, TFTP), Detection Strategy DET0416

Archived: 2026-04-05 13:24:38 UTC

AN1169

Detects FTP, SMB, or TFTP traffic initiated by suspicious processes like PowerShell, cmd.exe, or rundll32.exe—especially with large outbound file transfers or unbalanced traffic volume.

Log Sources

Mutable Elements

Field	Description
ProcessImageFilter	Limit to non-standard FTP clients or suspicious binaries (e.g., cmd, mshta)
DataFlowDirectionThreshold	Ratio of outbound:inbound bytes; e.g., >90% outbound
FilenamePattern	Suspicious file extensions or naming (e.g., .zip, .rar, random hash names)

AN1170

Detects usage of FTP, SCP, or TFTP by non-interactive shells or automation scripts transferring large data volumes to untrusted IPs.

Log Sources

Mutable Elements

Field	Description
TransferSizeThreshold	Bytes sent in FTP upload or SCP push
CommandLinePatternMatch	e.g., scp -r /var/log/* or ftp upload scripts

AN1171

Detects Automator, AppleScript, or Terminal executing curl, lftp, or TFTP for binary transfer to untrusted IPs or unusual ports.

Log Sources

Mutable Elements

Field	Description
FilePathAccessed	e.g., ~/Documents, ~/Library/logs/
NetworkPortAnomaly	Non-standard FTP/TFTP ports used (e.g., FTP over 443)

AN1172

Detects file movement or outbound TFTP/FTP transfers from ESXi host initiated via shell commands or injected scripts, particularly from scratch partitions or /tmp.

Log Sources

Mutable Elements

Field	Description
TransferTargetDomainOrIP	Public IPs or domains not belonging to known ESXi mgmt infra
SourceDirectoryFilter	Monitor transfers from /tmp/, /etc/, /vmfs/volumes/

AN1173

Detects internal hosts generating large outbound FTP/TFTP/SMB sessions to external IPs, or file transfers using non-standard ports and application mismatches (e.g., FTP over port 80).

Log Sources

Mutable Elements

Field	Description
AppLayerProtocolMatch	e.g., FTP/SMB observed over uncommon ports
OutboundDataRateThreshold	Bytes transferred outside trusted subnets >100MB
