Detection Strategy for Spearphishing Attachment across OS Platforms, Detection Strategy DET0236

Archived: 2026-04-05 16:40:53 UTC

AN0655

Detection of spearphishing attachments by correlating suspicious email delivery with subsequent file creation and abnormal process execution (e.g., Office spawning PowerShell or CMD). Behavior chain includes inbound email metadata → attachment stored on disk → process execution → outbound network activity.

Log Sources

Mutable Elements

Field	Description
AttachmentExtensions	List of high-risk extensions to monitor (e.g., .exe, .js, .vbs, .docm, .xlsm).
SuspiciousParentChildPairs	Process lineage patterns considered malicious (e.g., winword.exe → powershell.exe).
TimeWindow	Correlation window between email receipt, file creation, and process execution.

AN0656

Phishing attachments executed on Linux systems are detected by linking email logs to file creation in mail directories and subsequent suspicious process execution. Look for unexpected binaries or scripts spawned from user mail directories and anomalous outbound network activity.

Log Sources

Mutable Elements

Field	Description
AttachmentStoragePaths	Monitored directories for email attachments (e.g., /var/mail, ~/Maildir, ~/Downloads).
ScriptInterpreters	List of interpreters to monitor when spawned by mail clients (e.g., bash, python, perl).

AN0657

Phishing attachment detection on macOS through correlation of Mail app logs, file creation in user directories, and abnormal process execution (e.g., Preview.app or Mail.app spawning Terminal or scripting binaries). Network traffic after attachment interaction is also monitored.

Log Sources

Mutable Elements

Field	Description
ExecutionDelayThreshold	Time delay between attachment download and execution considered suspicious.
SuspiciousParentApps	Parent processes expected to rarely spawn child processes (e.g., Mail.app, Preview.app).
