Detection Strategy for Spearphishing via a Service across OS Platforms, Detection Strategy DET0115

Archived: 2026-04-02 12:19:54 UTC

AN0320

Inbound spearphishing attempts delivered via third-party services (e.g., Gmail, LinkedIn messages) leading to malicious file downloads or browser-initiated script execution. Defender view includes correlation of external service logins, unexpected file write operations, and suspicious descendant processes spawned from productivity or browser applications.

Log Sources

Mutable Elements

Field	Description
MonitoredServices	List of third-party services (e.g., Gmail, LinkedIn, Dropbox) relevant to the organization’s threat profile.
SuspiciousProcessPatterns	Process lineage and parent-child execution relationships considered abnormal (e.g., outlook.exe → powershell.exe).
TimeWindow	Correlates file creation and outbound connection activity within a tunable time period after message receipt.

AN0321

Use of non-enterprise email or messaging services in Thunderbird, Evolution, or browsers leading to suspicious file downloads and subsequent execution. Defender view includes browser-initiated downloads of unexpected content and shell or interpreter processes launched post-download.

Log Sources

Mutable Elements

Field	Description
BrowserProcesses	Configured list of browsers or email clients to monitor (e.g., firefox, chromium, thunderbird).
PhishingIndicators	Custom regex rules for suspicious URL patterns, file extensions, or encoded links.

AN0322

Phishing attempts via iCloud Mail, Gmail, or social media apps accessed on macOS systems. Defender view includes Mail.app or Safari downloads of files followed by osascript, Terminal, or abnormal child process execution.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	macos:unifiedlog	Received messages containing embedded links or attachments from non-enterprise services
Process Creation (DC0032)	macos:unifiedlog	Execution of osascript, bash, or Terminal initiated from Mail.app or Safari
Network Traffic Content (DC0085)	macos:unifiedlog	Suspicious outbound HTTPS requests to domains flagged as newly registered or untrusted after spearphishing message interaction

Mutable Elements

Field	Description
CertificateChecks	Flagging mismatched or self-signed certificates during outbound connections initiated after spearphishing messages.
ExecutionDelay	Window of time between attachment download and subsequent suspicious execution.
