Detection Strategy for Phishing across platforms., Detection Strategy DET0070

Archived: 2026-04-05 16:02:19 UTC

AN0188

Unusual inbound email activity where attachments or embedded URLs are delivered to users followed by execution of new processes or suspicious document behavior. Detection involves correlating email metadata, file creation, and network activity after a phishing message is received.

Log Sources

Mutable Elements

Field	Description
SuspiciousFileTypes	Attachment types considered high risk (e.g., .exe, .js, .vbs, .scr, macro-enabled docs).
AllowedSenders	Whitelist of known trusted senders to reduce false positives.

AN0189

Monitor for malicious payload delivery through phishing where attachments or URLs in email clients (e.g., Thunderbird, mutt) result in unusual file creation or outbound network connections. Focus on correlation between mail logs, file writes, and execution activity.

Log Sources

Mutable Elements

Field	Description
MonitoredMailPaths	System or user directories where emails/attachments are stored.
AttachmentHashBaseline	Known good hashes for common business document templates.

AN0190

Detection of phishing through anomalous Mail app activity, such as attachments saved to disk and immediately executed, or Safari/Preview launching URLs and files linked from email messages. Correlate UnifiedLogs events with subsequent process execution.

Log Sources

Mutable Elements

Field	Description
SuspiciousDomains	List of domains known for phishing activity or suspicious sender infrastructure.
ExecutionDelayWindow	Time threshold between file save and execution considered suspicious.

AN0191

Phishing via Office documents containing embedded macros or links that spawn processes. Detection relies on correlating Office application logs with suspicious child process execution and outbound network connections.

Log Sources

Mutable Elements

Field	Description
ParentProcessList	Parent processes expected to execute child processes (e.g., Office apps).
MacroExecutionThreshold	Threshold for number of macros executed before raising alerts.

AN0192

Phishing attempts targeting IdPs often manifest as anomalous login attempts from suspicious email invitations or fake SSO prompts. Detection correlates login flows, MFA bypass attempts, and anomalous geographic patterns following phishing email delivery.

Log Sources

Data Component	Name	Channel
Logon Session Creation (DC0067)	azure:signinlogs	Failed MFA attempts, unusual conditional access triggers, login attempts from unexpected IP ranges

Mutable Elements

Field	Description
GeoAnomalyThreshold	Allowed distance/time delta between user sign-ins.
MFABypassIndicators	Signals of repeated or anomalous MFA failures linked to phishing campaigns.

AN0193

Phishing delivered via SaaS services (chat, collaboration platforms) where messages contain malicious URLs or attachments. Detect anomalous link clicks, suspicious file uploads, or token misuse after SaaS-based phishing attempts.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	saas:collaboration	MessagePosted: Suspicious links or attachment delivery via collaboration tools (Slack, Teams, Zoom)

Mutable Elements

Field	Description
MonitoredSaaSApps	Scope of SaaS platforms under phishing monitoring.
LinkInspectionPolicy	Threshold for auto-expansion and detonation of URLs sent in SaaS messages.
