

# Detection Strategy for Spearphishing Links, Detection Strategy DET0107

Archived: 2026-04-05 12:43:52 UTC

## AN0298

Correlation of inbound emails with embedded links followed by user-driven browser navigation to suspicious or obfuscated domains. Detection chain includes malicious URL in email → user click recorded in Office logs → browser process spawning unusual child processes (e.g., PowerShell, cmd) or download activity.

### Log Sources

### Mutable Elements

Field	Description
SuspiciousTLDs	List of monitored top-level domains commonly abused in phishing (e.g., .xyz, .top, .tk).
URLShortenerDomains	Domains like bit.ly, tinyurl.com flagged for deeper expansion/inspection.
ClickToExecutionWindow	Time threshold between URL click and suspicious process execution.

## AN0299

Detection of spearphishing links through mail logs and browser activity. Behavior includes email with suspicious URLs → user click recorded in mail/web proxy logs → shell or interpreter launched from browser process.

### Log Sources

### Mutable Elements

Field	Description
MonitoredBrowsers	List of browser processes to monitor (e.g., firefox, chrome, chromium).
PhishingIndicators	Custom regex patterns for detecting obfuscated or IDN homograph URLs.

## AN0300

Correlation of Mail.app logs with Safari/Chrome activity. Suspicious behavior includes email links → Safari/Chrome accessing newly registered or lookalike domains → osascript or Terminal spawned unexpectedly.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
CertificateAnomalies	Flag self-signed or mismatched TLS certificates from spearphishing domains.
ExecutionDelayThreshold	Suspicious delay between URL click and malicious process spawn.

**AN0301**

Detection of OAuth consent phishing or malicious login attempts initiated through spearphishing links. Behavior chain includes inbound email with OAuth URL → consent page visited → unusual token grants logged in IdP logs.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
AllowedApps	Whitelisted apps permitted for OAuth consent grants.
AnomalousConsentPatterns	Patterns of consent from unusual geographies, devices, or unapproved applications.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0107#AN0300>