Detection of Phishing for Information, Detection Strategy DET0823

Archived: 2026-04-05 16:36:47 UTC

AN1955

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
Depending on the specific method of phishing, the detections can vary. Monitor for suspicious email activity, such as numerous accounts receiving messages from a single unusual/unknown sender. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[1][2]
When it comes to following links, monitor for references to uncategorized or known-bad sites. URL inspection within email (including expanding shortened links) can also help detect links leading to known malicious sites.
Monitor social media traffic for suspicious activity, including messages requesting information as well as abnormal file or data transfers (especially those involving unknown, or otherwise suspicious accounts).

Monitor call logs from corporate devices to identify patterns of potential voice phishing, such as calls to/from known malicious phone numbers.
Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

Log Sources