Detection of Spearphishing Attachment, Detection Strategy DET0865

Archived: 2026-04-05 18:36:09 UTC

AN1997

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.
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]
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)).

Log Sources
