Detection of Spearphishing Service, Detection Strategy DET0821

Archived: 2026-04-05 14:36:26 UTC

AN1953

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). Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.
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 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

Source: https://attack.mitre.org/detectionstrategies/DET0821