Detection of Spearphishing Link, Detection Strategy DET0878

Archived: 2026-04-05 16:14:11 UTC

AN2010

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 for references to uncategorized or known-bad sites. URL inspection within email (including expanding shortened links and identifying obfuscated URLs) can also help detect links leading to known malicious sites.[3]

Furthermore, monitor browser logs for homographs in ASCII and in internationalized domain names abusing different character sets (e.g. Cyrillic vs Latin versions of trusted sites).
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), leveraging SSL/TLS inspection for encrypted traffic, 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)).

Furthermore, monitor network traffic for homographs via the use of internationalized domain names abusing different character sets (e.g. Cyrillic vs Latin versions of trusted sites). Also monitor and analyze traffic patterns and packet inspection for indicators of cloned websites. For example, if adversaries use HTTrack to clone websites, `Mirrored from (victim URL)` may be visible in the HTML section of packets.

Log Sources
