Detection of Masquerading, Detection Strategy DET0725

Archived: 2026-04-05 14:11:00 UTC

Analytics

- ICS

AN1858

Monitor for newly constructed services/daemons that may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.
Monitor for changes made to files outside of an update or patch that may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.
Monitor for file names that are mismatched between the file name on disk and that of the binary's metadata. This is a likely indicator that a binary was renamed after it was compiled. For added context on adversary procedures and background see Masquerading and applicable sub-techniques.
Monitor executed commands and arguments that may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.[1]
Monitor for changes made to scheduled jobs that may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.
Monitor for changes made to services that may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.
Collect file hashes. Monitor for file names that do not match their expected hash. Perform file monitoring. Files with known names but in unusual locations are suspect. Look for indications of common characters that may indicate an attempt to trick users into misidentifying the file type, such as a space as the last character of a file name or the right-to-left override characters"\u202E", "[U+202E]", and "%E2%80%AE". For added context on adversary procedures and background see Masquerading and applicable sub-techniques.
Monitor for newly constructed scheduled jobs that may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.

Log Sources

References

1. Carr, N.. (2018, October 25). Nick Carr Status Update Masquerading. Retrieved September 12, 2024.