Detect Kerberos Ccache File Theft or Abuse (T1558.005), Detection Strategy DET0024

Archived: 2026-04-05 16:02:49 UTC

AN0069

Detects unauthorized access, copying, or modification of Kerberos ccache files (krb5cc_%UID% or krb5.ccache) in /tmp or custom paths defined by KRB5CCNAME. Correlates file access with suspicious processes (e.g., credential dumping tools) and subsequent anomalous Kerberos authentication requests from non-standard processes.

Log Sources

Data Component	Name	Channel
File Access (DC0055)	auditd:SYSCALL	open: File access attempt on /tmp/krb5cc_* or /tmp/krb5.ccache
Process Creation (DC0032)	auditd:SYSCALL	execve: Execution of klist, kinit, or tools interacting with ccache outside normal user context

Mutable Elements

Field	Description
CcachePathBaseline	Expected directories or environment variable (KRB5CCNAME) paths for ccache files in the environment.
AllowedProcesses	Baseline list of processes legitimately interacting with ccache (e.g., klist, kinit).
TimeWindow	Correlation window for linking file access, process execution, and Kerberos requests.

AN0070

Detects abnormal interaction with memory-based Kerberos ccache (API:{uuid}) or file-based overrides. Focus on processes attempting to enumerate or extract Kerberos tickets outside of built-in utilities. Detects use of open-source tools (e.g., Bifrost, modified Mimikatz ports) that interact with the Kerberos framework APIs.

Log Sources

Data Component	Name	Channel
File Access (DC0055)	macos:unifiedlog	Kerberos framework calls to API:{uuid} cache outside normal process lineage
Process Creation (DC0032)	macos:osquery	Execution of non-standard binaries accessing Kerberos APIs

Mutable Elements

Field	Description
KerberosAPIProcessBaseline	Expected processes using the Kerberos framework (e.g., loginwindow, kinit).
SuspiciousBinaryList	List of tools or binaries not normally expected to query Kerberos ccache entries.
TimeWindow	Window to link suspicious process activity with Kerberos authentication anomalies.
