Post-Credential Dump Password Cracking Detection via Suspicious File Access and Hash Analysis Tools, Detection Strategy DET0105

Archived: 2026-04-05 12:48:03 UTC

AN0292

Use of hash-cracking tools (e.g., John the Ripper, Hashcat) after credential dumping, combined with high CPU usage or GPU invocation via unsigned binaries accessing password hash files

Log Sources

Mutable Elements

Field	Description
HashToolName	Match execution against known cracking toolnames like hashcat.exe, john.exe, etc.
FilePathIndicators	Watch for access to common hash dump locations (e.g., SAM, SYSTEM, NTDS.dit)
ExecutionContext	Run context: local interactive user vs. scheduled task or remote session

AN0293

Execution of hash cracking binaries or scripts (e.g., john, hashcat) following access to shadow file or dumped hashes

Log Sources

Mutable Elements

Field	Description
ShadowAccessPattern	Access to /etc/shadow or known dumped hash files
CrackingBinaryPath	Tool path or name associated with hash cracking
CPUUsageThreshold	Sustained CPU load post-credential dump can be an indicator

AN0294

Unsigned or scripting-based processes invoking password cracking binaries or accessing hashed credential artifacts post-login

Log Sources

Mutable Elements

Field	Description
UnsignedBinaryPath	Path to untrusted binaries launched by user
UserPrivilegeLevel	Helps distinguish between system and user-launched activity

AN0295

Sudden valid logins from accounts that previously had credentials dumped but had not authenticated successfully in the past; correlated with timeline of suspected hash cracking

Log Sources

Mutable Elements

Field	Description
PostDumpTimeWindow	Detection window after credential dumping to watch for successful logins
LoginLocationRisk	Use IP/geolocation risk scoring to flag unusual access

AN0296

Offline cracking inferred by subsequent successful CLI or web-based authentications into routers or switches from previously dumped accounts

Log Sources

Mutable Elements

Field	Description
LogonTimeCorrelation	Window to link credential theft and reuse
SourceDeviceTag	Filters based on where cracking may have occurred externally

---

Source: https://attack.mitre.org/detectionstrategies/DET0105#AN0295