Detect Access and Decryption of Group Policy Preference (GPP) Credentials in SYSVOL, Detection Strategy DET0381

Archived: 2026-04-05 13:40:29 UTC

Analytics

- Windows

AN1075

Correlates file enumeration of XML files in the SYSVOL share with suspicious process execution that decodes or reads encrypted credentials embedded in Group Policy Preference files (e.g., Get-GPPPassword.ps1, gpprefdecrypt.py, Metasploit). Detects abnormal access to \DOMAIN\SYSVOL combined with XML file parsing or decryption logic.

Log Sources

Mutable Elements

Field	Description
UserContext	Tune to exclude authorized admin users or domain controllers accessing SYSVOL
TimeWindow	Adjust for correlation timing between file access and script execution
KnownToolsSignature	Extend to include known GPP parsing tool names or script hashes
HostType	Distinguish between expected access from DCs vs. lateral movement from workstations