Detection of Credential Harvesting via Web Portal Modification, Detection Strategy DET0480

Archived: 2026-04-05 16:53:14 UTC

AN1320

Detects unauthorized modifications to login-facing web server files (e.g., index.php, login.js) typically tied to VPN, SSO, or intranet portals. Correlates suspicious file changes with remote access artifacts or web shell behavior.

Log Sources

Mutable Elements

Field	Description
MonitoredFilePaths	Target login-related files (e.g., /var/www/html/login.php) for integrity monitoring
TimeWindow	Tune detection to correlate file edits and web access within a short duration

AN1321

Detects tampering of IIS-based login pages (e.g., default.aspx, login.aspx) tied to VPN, OWA, or SharePoint via script injection or unexpected editor processes modifying web roots.

Log Sources

Mutable Elements

Field	Description
FilePath	Define path to monitored IIS web root (e.g., C:\inetpub\wwwroot\login.aspx)
ProcessName	Exclude legitimate updates (e.g., msdeploy.exe) and alert on suspicious editors (e.g., notepad.exe, certutil.exe)

AN1322

Detects unauthorized changes to locally hosted login pages on macOS (common in developer VPN environments) and links file edits to cron jobs, background scripts, or SUID binaries.

Log Sources

Mutable Elements

Field	Description
WebRootPath	Specify custom web service directories (e.g., /Library/WebServer/Documents/)
AnomalousProcess	Alert on web root changes from non-web processes or scripts

---

Source: https://attack.mitre.org/detectionstrategies/DET0480#AN1320