Internal Website and System Content Defacement via UI or Messaging Modifications, Detection Strategy DET0082

Archived: 2026-04-05 15:56:10 UTC

AN0229

Adversary modifies internal UI messages (e.g., login banners, desktop wallpapers) or hosted intranet web pages by creating or altering content files using scripts or unauthorized access. Often preceded by privilege escalation or web shell deployment.

Log Sources

Mutable Elements

Field	Description
FilePathPattern	Location of web content or system UI config files that may vary across deployments (e.g., %SystemRoot%\Web, %APPDATA%\wallpaper.jpg)
TimeWindow	Allowed hours for file/content modification events; defacement likely occurs during off-hours
UserContext	System or domain accounts used to perform the modifications may be anomalous

AN0230

Adversary leverages root or sudo access to alter system banners, web content directories (e.g., /var/www/html), or login configurations (/etc/issue). File creation or overwrites may coincide with suspicious script execution or cron job activity.

Log Sources

Mutable Elements

Field	Description
TargetDirectories	Paths like /var/www/html, /etc/issue, or /etc/motd may vary across distros
UserContext	Non-web-admin users modifying site content or banners should be rare
TimeWindow	Defacement often happens outside normal maintenance hours

AN0231

Modification of user desktop backgrounds, login screen messages, or system banners by adversaries using admin privileges or script execution. May coincide with tampering in /Library/Desktop Pictures/ or use of AppleScript.

Log Sources

Mutable Elements

Field	Description
ScriptNames	Uncommon scripts like AppleScript variants or osascript for wallpaper changes
UserContext	Normal users should not alter global visual settings

AN0232

Adversary modifies ESXi host login banner or MOTD file (/etc/motd), either through SSH or host console access. May involve configuration file overwrite or API calls from compromised vSphere clients.

Log Sources

Mutable Elements

Field	Description
LoginBannerFilePath	Target file paths (e.g., /etc/motd) may be changed via symbolic link or override
AccessOrigin	ESXi hostd vs. SSH-based defacement origin may affect visibility

---