Defacement: Internal Defacement, Sub-technique T1491.001 - Enterprise

Archived: 2026-04-05 12:49:39 UTC

ID	Name	Analytic ID	Analytic Description
DET0082	Internal Website and System Content Defacement via UI or Messaging Modifications	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.
		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.
		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.
		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.