

Defacement, Technique T1491 - Enterprise

Archived: 2026-04-02 11:34:39 UTC

ID	Name	Analytic ID	Analytic Description
DET0238	Defacement via File and Web Content Modification Across Platforms	AN0662	Adversary modifies website or application-hosted content via unauthorized file changes or script injections, often by exploiting web servers or CMS access.
		AN0663	Adversary gains shell access or uploads a malicious script to deface hosted web content in Nginx, Apache, or other services.
		AN0664	Adversary modifies internal or external site content through manipulated application bundles, hosted content, or web server configs.
		AN0665	Adversary defaces internal VM-hosted portals or web UIs by modifying static content on datastore-mounted paths.
		AN0666	Adversary uses compromised instance credentials or web application access to deface content hosted in S3 buckets, Azure Blob Storage, or GCP Buckets.

Source: <https://attack.mitre.org/techniques/T1491>