

# Behavioral Detection of External Website Defacement across Platforms, Detection Strategy DET0590

Archived: 2026-04-05 17:30:06 UTC

## AN1622

Adversary modifies externally-facing web content by accessing and overwriting hosted HTML/JS/CSS files, typically following web shell deployment, credential abuse, or exploitation of web application vulnerabilities.

### Log Sources

### Mutable Elements

Field	Description
target_directory	Web root folder varies by environment, e.g., C:\inetpub\wwwroot
UserContext	May vary based on which service account hosts the website
TimeWindow	Time between webshell upload and file overwrite may vary

## AN1623

Adversary compromises a Linux-based web server and modifies hosted web files by exploiting upload vulnerabilities, remote code execution, or replacing index.html via SSH/webshell.

### Log Sources

### Mutable Elements

Field	Description
web_root	May differ (e.g., /var/www/html, /srv/http, etc.)
payload_hash	Adversary content hash may change across campaigns
UserContext	Can range from apache/nginx user to root if escalated

## AN1624

Adversary modifies web-facing content on macOS via web development environments like MAMP or misconfigured Apache instances, typically with access to the hosting user account or via persistence tools.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
web_root_dir	May include ~/Sites or custom Apache paths
editor_name	Text editor or script modifying the files may vary (e.g., nano, VS Code)

**AN1625**

Adversary modifies content in cloud-hosted websites (e.g., AWS S3-backed, Azure Blob-hosted sites) by gaining access to management consoles or APIs and uploading altered HTML/JS files.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
bucket_name	Website bucket name varies per org
region	Adversary may target multi-region failover setups
IAMRole	Attack may leverage stolen cross-account roles or elevated policies

---

Source: <https://attack.mitre.org/detectionstrategies/DET0590>