Web Shell Detection via Server Behavior and File Execution Chains, Detection Strategy DET0394

Archived: 2026-04-05 13:57:10 UTC

AN1108

Unexpected file creation in web directories followed by web server processes (e.g., w3wp.exe) spawning command shells or script interpreters (e.g., cmd.exe, powershell.exe)

Log Sources

Mutable Elements

Field	Description
WebRootPath	Custom web server directory depending on IIS or third-party hosting environment
ParentProcess	Different server binaries (e.g., php-cgi.exe, apache.exe) that may launch scripts

AN1109

File creation of unauthorized script (e.g., .php, .sh) in /var/www/html followed by execution of unexpected system utilities (e.g., curl, bash, nc) by apache/nginx

Log Sources

Mutable Elements

Field	Description
WebRootPath	Web server root varies by distro and hosting configuration
PayloadEntropyThreshold	Base64 or XOR encoded shells may exceed this value
TimeWindow	Correlate file creation with process spawn within X seconds

AN1110

Web servers (e.g., httpd) spawning abnormal processes post file upload into /Library/WebServer/Documents or /usr/local/var/www

Log Sources

Mutable Elements

Field	Description
InterpreterName	Adversary may use different scripting environments
ExecutionParent	Not all web servers are named httpd; may differ in custom deployments

---

Source: https://attack.mitre.org/detectionstrategies/DET0394#AN1109