Detection Strategy for T1505 - Server Software Component, Detection Strategy DET0547

Archived: 2026-04-05 16:15:09 UTC

AN1507

Installation of malicious IIS/Apache/SQL server modules that later execute command-line interpreters or establish outbound connections.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time delta between module install and process execution (e.g., persistence delay).
ParentProcessName	Custom server wrapper processes or renamed webserver processes may require tuning.

AN1508

Abuse of extensible server modules (e.g., Apache, Nginx, Tomcat) to load rogue plugins that initiate bash, connect to C2, or spawn reverse shells.

Log Sources

Mutable Elements

Field	Description
ServerBinaryPath	Alternate install paths like /opt/httpd or user-compiled binaries
OutboundPortRange	Tunable to match expected versus suspicious outbound traffic patterns

AN1509

Malicious use of webserver plugins (e.g., for nginx, PHP, Node.js) that execute AppleScript or open network sockets.

Log Sources

Mutable Elements

Field	Description
ParentBinaryPath	If homebrew or manually compiled nginx/httpd used, baseline accordingly.

AN1510

Use of ESXi web interface plugins or vSphere extensions to embed persistent malicious scripts or services.

Log Sources

Mutable Elements

Field	Description
PluginVendorName	Whitelist known vendor plug-in names for extension correlation
AccessVector	Limit exposure of plugin installation via HTTPS or SSH
