Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), Detection Strategy DET0080

Archived: 2026-04-05 18:00:54 UTC

AN0219

Adversary sends crafted HTTP/S (or other service) input to an Internet-facing app (IIS/ASP.NET, API, device portal). Chain: (1) abnormal request patterns to public endpoint → (2) elevated 4xx/5xx or unusual methods/paths → (3) server process (w3wp.exe/other service) spawns shell/LOLbins or loads non-standard modules → (4) optional outbound callback from the host/container.

Log Sources

Mutable Elements

Field	Description
PublicVIPs	List of public IPs/hostnames that front apps; used to scope web log and Zeek/proxy data.
SuspiciousPatterns	Regex set for exploit-like inputs (../, union select, cmd=, ${jndi:, rO0AB (Java serialization), %00, ${env:}, ${${::-j}ndi}).
ErrorRateThreshold	Spike threshold for HTTP status 5xx/4xx per client or URI (e.g., >5 in 5m).
TimeWindow	Correlation horizon between request, error, process spawn, and egress (e.g., 15 minutes).
AllowedChildList	Known child processes of app pools (e.g., msbuild.exe in CI) to reduce false positives.

AN0220

Adversary exploits Apache/Nginx/app servers. Chain: (1) suspicious requests in access logs → (2) spike of 5xx or WAF blocks → (3) web server or interpreter (apache2/nginx/php-fpm/node/python) spawns /bin/sh, curl, wget, socat, or writes webshell → (4) outbound callback.

Log Sources

Mutable Elements

Field	Description
WebProcList	server/interpreter names to watch (apache2, httpd, nginx, php-fpm, uwsgi, gunicorn, node).
ChildToolList	post-exploitation binaries (sh, bash, curl, wget, python, perl, socat, nc).
BurstThreshold	Rate of errors/requests per src_ip/uri to flag reconnaissance/exploit spray.
TimeWindow	Exec/network correlation window.

AN0221

Adversary targets macOS-hosted public services (e.g., nginx, node). Chain: suspicious inbound request → service crash/5xx → service spawns shell or writes file → new outbound connection.

Log Sources

Mutable Elements

Field	Description
ServiceList	Names/paths of public daemons on macOS (httpd, nginx, node, java).
TimeWindow	Correlation window for request → exec → egress.

AN0222

Adversary exploits containerized app via ingress or service. Chain: (1) suspicious request in ingress/app logs → (2) container process spawns a shell/exec/sidecar (kubectl exec/docker exec) → (3) egress to Internet or metadata service (169.254.169.254).

Log Sources

Mutable Elements

Field	Description
IngressNamespaces	Namespaces that are Internet-facing.
MetadataEndpoints	Cloud metadata IPs/hostnames for exfil of credentials.
TimeWindow	Join period between ingress request and pod exec/egress.

AN0223

Adversary targets cloud-hosted public endpoints. Chain: (1) ALB/ELB/Cloud LB logs show exploit-like inputs or error spikes → (2) workload spawns shell or reaches metadata API → (3) egress to new external hosts.

Log Sources

Data Component	Name	Channel
Network Traffic Content (DC0085)	ALB:HTTPLogs	AWS ALB/ELB/GCP/Azure Application Gateway HTTP logs with unusual methods, long URIs, serialized payloads, 4xx/5xx bursts
Network Traffic Flow (DC0078)	AWS:VPCFlowLogs	VPC/NSG flow logs for pod/instance egress to Internet or metadata

Mutable Elements

Field	Description
LBProjects	Cloud accounts/subscriptions/regions to include.
ErrorBurst	5xx/4xx per client threshold.

AN0224

Adversary exploits exposed OpenSLP on ESXi or vCenter public endpoints. Chain: inbound request pattern to mgmt service → hostd/vpxd error/crash/restart → unexpected process behavior or datastore access → outbound callback.

Log Sources

Mutable Elements

Field	Description
MgmtCIDR	Only trusted admin networks should reach ESXi/vCenter.
TimeWindow	Join errors and inbound flows.

AN0225

Adversary exploits public admin services on routers/firewalls/switches. Chain: anomalous HTTP/SNMP/SmartInstall inputs → device syslog errors/restarts → config changes/CLI spawn → egress to attacker C2.

Log Sources

Mutable Elements

Field	Description
MgmtPorts	List of admin services to watch (8443, 443, 161/udp, 4786, 22).
TrustedAdmins	Admin source ranges to allow.
