Multi-Platform Behavioral Detection for Compute Hijacking, Detection Strategy DET0540

Archived: 2026-04-05 14:03:30 UTC

AN1489

Sustained execution of resource-intensive processes (e.g., cryptocurrency miners), often launched via scheduled tasks, WMI, or PowerShell. These processes frequently establish persistent external connections and attempt to evade detection using masqueraded or renamed binaries.

Log Sources

Mutable Elements

Field	Description
Image	The executable name of the miner or wrapper—can vary across campaigns.
DestinationIP	May differ depending on the mining pool or proxy server.
ParentProcessName	Useful for filtering known-good automation vs malicious task runners.

AN1490

Unusual long-running processes consuming high CPU cycles (e.g., via 'top' or 'ps') initiated via cron, shell scripts, or Docker. Connections to known mining pools or DNS over HTTPS usage as evasion.

Log Sources

Mutable Elements

Field	Description
CommandLine	The miner's execution path and options may vary by campaign.
CPUThreshold	Environment-specific definition of anomalous CPU usage.

AN1491

Persistent or background daemons (e.g., plist or launchd jobs) spawning high-CPU processes like xmrig or cpuminer. Outbound encrypted traffic to IPs/domains commonly used by mining proxies.

Log Sources

Mutable Elements

Field	Description
launchd.plist_label	May be disguised with benign-looking names.
DestinationDomain	Varying mining pool or obfuscated destination.

AN1492

Ephemeral or unauthorized container instantiation using public images (e.g., from DockerHub) that initiate high CPU usage shortly after startup. Often scheduled via Kubernetes or Docker socket abuse.

Log Sources

Mutable Elements

Field	Description
ImageSource	May vary depending on where the image is pulled from (registry or custom URL).
Namespace	Helps differentiate attacker-created namespaces.

AN1493

Unauthorized instance creation in unmonitored or unused regions. Burst of compute-intensive jobs in spot instances or sudden spike in resource usage in legitimate VMs.

Log Sources

Mutable Elements

Field	Description
Region	Adversaries may deploy resources in rarely used or misconfigured regions.
TagKey	Used to evade detection with benign-looking tags or names.
