Detection Strategy for T1542 Pre-OS Boot, Detection Strategy DET0278

Archived: 2026-04-05 12:51:28 UTC

AN0774

Unusual modification of boot records (MBR, VBR) or EFI partitions not associated with legitimate patch cycles or OS upgrades. Registry or WMI events associated with firmware update tools executed from unexpected parent processes. API calls (e.g., DeviceIoControl) writing directly to raw disk sectors. Subsequent abnormal boot configuration changes followed by unsigned driver loads.

Log Sources

Mutable Elements

Field	Description
AllowedFirmwareUpdateTools	Legitimate vendor tools or processes authorized to modify firmware or boot records.
TimeWindow	Correlating boot-sector modification with subsequent reboot events.
EntropyThreshold	Heuristic threshold for detecting obfuscated/packed boot code.

AN0775

Detection of writes to /boot or EFI directories outside of expected package manager updates. Monitoring kernel log and auditd events for attempts to overwrite bootloader binaries (e.g., grub, shim). Unexpected execution of efibootmgr or dd writing to /dev/sdX devices followed by boot parameter changes.

Log Sources

Mutable Elements

Field	Description
PackageManagerUpdateWhitelist	Allowlist of legitimate grub/shim updates via apt, yum, or rpm.
FilesystemPaths	Directories (e.g., /boot/efi, /boot/grub) monitored for unauthorized modification.

AN0776

Abnormal modification of EFI firmware binaries in /System/Library/CoreServices/ or NVRAM parameters not associated with OS updates. Unified logs capturing calls to bless or nvram commands executed from untrusted parent processes. Sudden unsigned kext loads after EFI variable tampering.

Log Sources

Mutable Elements

Field	Description
AllowedBootUtilities	Known Apple-signed processes responsible for firmware updates.
BootParamBaseline	Baseline set of allowed NVRAM boot parameters for anomaly detection.

AN0777

Unexpected firmware image uploads via TFTP/FTP/SCP. Configuration changes modifying boot image pointers. Logs showing boot variable redirection to non-standard images. Anomalous reboots immediately following firmware changes not tied to patch schedules.

Log Sources

Mutable Elements

Field	Description
ApprovedFirmwareHashes	Known good firmware image hashes allowed for boot.
MaintenanceWindows	Timeframes during which firmware updates are expected.
