Detection Strategy for SSH Key Injection in Authorized Keys, Detection Strategy DET0126

Archived: 2026-04-05 13:19:45 UTC

AN0350

Adversary attempts to gain persistence by modifying ~/.ssh/authorized_keys via shell, text editor, echo or redirected output.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Temporal window to correlate file writes and suspicious process launches (e.g., <60s)
UserContext	Expected user-to-process correlation (e.g., root writing to non-root authorized_keys)
TargetPath	Custom SSH path or user home variation (e.g., /etc/skel/.ssh/)

AN0351

Insertion of public keys into authorized_keys using bash/zsh or editor tools, correlated with suspicious process ancestry.

Log Sources

Mutable Elements

Field	Description
ParentProcess	Track unusual parent process writing to SSH config (e.g., curl -> bash)
InteractiveSessionFlag	Flag whether shell session was interactive (normal) or spawned remotely (potential abuse)

AN0352

Abuse of cloud metadata APIs or CLI to push SSH public keys to authorized_keys of virtual machines.

Log Sources

Mutable Elements

Field	Description
MetadataFieldName	Custom metadata field (e.g., ssh-keys or custom-key)
AccountType	Was it an admin, service principal, or automation user initiating?
TargetRoleEscalation	Privilege level of the VM account receiving the key

AN0353

Direct modification of /etc/ssh/keys-/authorized_keys or enabling SSH in sshd_config to support public key auth.

Log Sources

Mutable Elements

Field	Description
SSHConfigPath	Could be modified SSH path in hypervisor
ESXiShellActivity	Whether shell was enabled beforehand via DCUI or API

AN0354

Use of command-line like `ip ssh pubkey-chain` to bind SSH keys to privileged accounts on routers or switches.

Log Sources

Mutable Elements

Field	Description
CLIUserRole	Was the role allowed to push persistent config changes?
DeviceModel	Variations in syntax or log behavior across device OS
