Remote Desktop Software Execution and Beaconing Detection, Detection Strategy DET0259

Archived: 2026-04-02 11:41:04 UTC

AN0714

Adversary installation or use of RMM software (e.g., TeamViewer, AnyDesk, ScreenConnect) followed by outbound beaconing or remote session establishment

Log Sources

Mutable Elements

Field	Description
Image	RMM software can vary; defenders should update rules to account for additional binaries (e.g., ConnectWise, Zoho Assist)
DestinationPort	RMM software may use configurable or random high ports outside of standard (e.g., 7070, 5650)
ParentImage	Expected parent process may vary in different enterprise contexts
TimeWindow	Correlation window for install-to-beacon or process-to-network event should match operational environment

AN0715

Execution of known or custom VNC/remote desktop daemons or tunneling agents that initiate external communication after launch

Log Sources

Mutable Elements

Field	Description
binary_name	Custom-compiled or renamed VNC servers (e.g., x11vnc, tightvncserver) may require local tuning
OutboundIPRange	Destination IP or ASN may shift depending on geolocation of cloud-hosted RMM backends

AN0716

Initiation of remote desktop sessions via AnyDesk, TeamViewer, or Chrome Remote Desktop accompanied by unexpected user logins or system modifications

Log Sources

Mutable Elements

Field	Description
process_signature	App may be notarized and signed differently depending on distribution method (App Store vs .pkg)
sandbox_exception	If the remote desktop tool circumvents sandbox, it may produce additional telemetry in local TCC logs

---