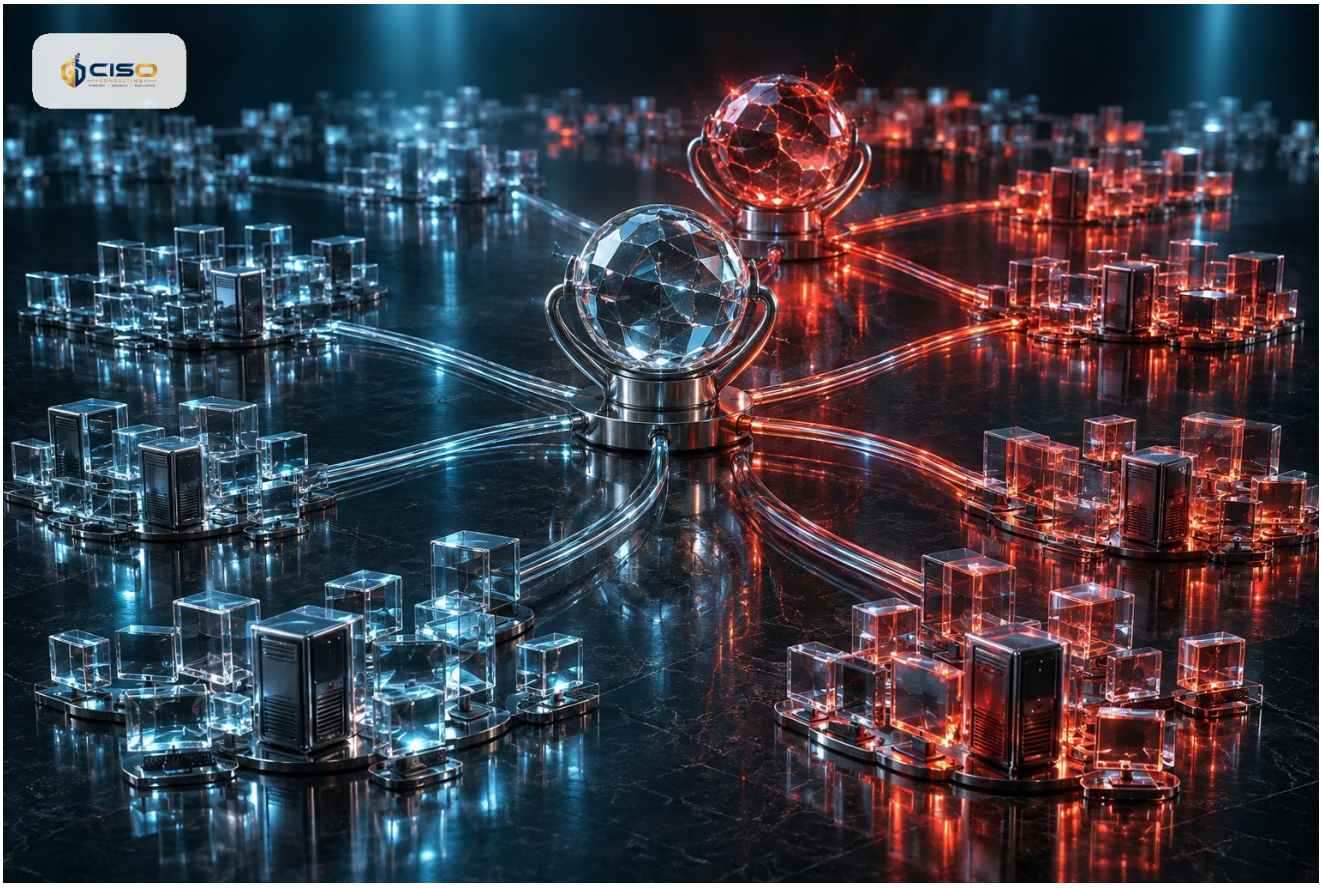
ScreenConnect campaign compromises MSPs and spreads rogue remote-access clients to customers



ConnectWise and Huntress report an active campaign abusing ScreenConnect at managed service providers to install rogue remote-access clients on customer devices. Huntress counts six MSPs and 286+ endpoints across 47 organizations, and the figures are rising.

- Huntress tracks six compromised MSPs and 286+ endpoints across 47 organizations, with numbers still rising.
- Attackers use ScreenConnect's Run Command feature to install rogue ScreenConnect clients outside the MSP's own environment.
- Huntress describes the activity as abuse of legitimate functionality, not a software vulnerability; initial access points to compromised credentials or hijacked operator sessions.
- ConnectWise disabled five third-party extensions across about 400 cloud partner environments;

> on-premises customers must disable them manually.
>
> - Technician workstations may be compromised during interactive sessions with infected devices; ConnectWise is still confirming these reports.

ConnectWise is investigating an active campaign in which attackers use compromised ScreenConnect environments at managed service providers (MSPs) to place rogue remote-access clients on customer devices. Huntress first detected the activity and reports six compromised MSPs and more than 286 endpoints across 47 organizations, with the count still growing.

What is happening

According to Huntress, the attackers use ScreenConnect's Run Command function to install rogue ScreenConnect clients on managed endpoints. This gives them remote access that sits outside the legitimate provider's environment. Huntress also warns of a more serious technique: a technician's workstation may be compromised when the technician opens a session with an infected customer device. ConnectWise says such reports are still being confirmed, and how the spread occurs has not been explained publicly.

Huntress describes the activity as abuse of legitimate functionality rather than exploitation of a vulnerability. It has not established how attackers enter MSP environments, but its telemetry points to compromised credentials or hijacked operator sessions. Sequential tags used by the attackers suggest other MSPs may have been affected earlier.

ConnectWise response

ConnectWise confirmed unauthorized access to ScreenConnect partner accounts. As a precaution it disabled five third-party extensions (Labtech Plus, RMM Plus, RMM+, RMM Plus Password Link and RMM+ Password Link) across about 400 partner environments. It stresses that having them installed does not prove compromise, and that disabling them does not remove software or access already in place. On-premises customers must disable the extensions themselves and should not re-enable them until further guidance is issued.

Implications

Organizations that rely on an MSP should treat this as a third-party risk event. Huntress has published indicators of compromise, including rogue client IDs and attacker infrastructure, which security teams can use for hunting.

What to do now

1. Ask your MSPs in writing whether they use ScreenConnect and whether any of the five named extensions are installed, and request confirmation of their investigation status.

2. If you run on-premises ScreenConnect, disable the five extensions manually and do not re-enable them until ConnectWise issues guidance.
3. Review authentication logs, extension installation records, administrative activity, Run Command history and Toolbox records, even if no alerts have fired.
4. Hunt for the published indicators (rogue client IDs, attacker domains and IPs, listed file names) across endpoints and network logs.
5. Avoid interactive ScreenConnect sessions with devices suspected of compromise; investigate them with separate security tools.
6. Reset credentials and review active operator sessions for ScreenConnect accounts, and confirm MFA is enforced for MSP access.