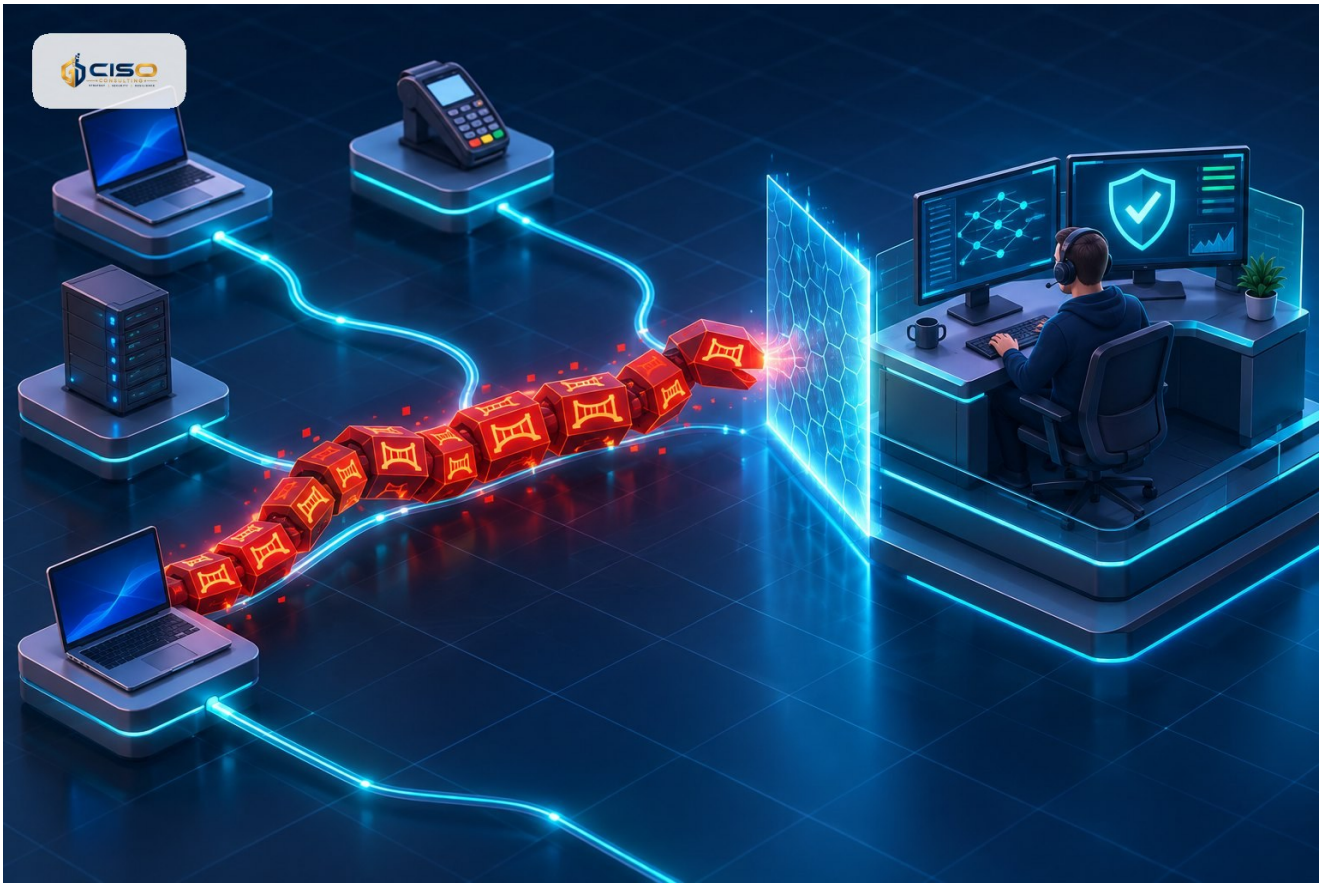
SCKit malware in ScreenConnect attacks tries to spread from customer devices to MSP technicians



A worm-like toolkit named SCKit was used in recent ScreenConnect attacks on MSPs. Researchers have not seen its spread succeed, but MSPs are urged to update clients and review activity.

- SCKit is a set of 16 scripts and components built to keep remote access and spread between systems managed through ScreenConnect.
- It tries to exploit CVE-2026-84869, a client-side file-transfer flaw patched in ScreenConnect 26.6.5, to run code on a technician's workstation.
- Huntress and Blackpoint Cyber have not seen successful exploitation; Blackpoint's test against a patched client failed.
- The wider attacks hit at least 288 endpoints across 48 organizations within 90 minutes, likely via

RMM+ versions 1.0.31 and 1.0.32.

- ConnectWise disabled five third-party extensions across about 400 partner environments, noting this does not imply compromise.

Researchers at Huntress and Blackpoint Cyber have analysed SCKit, a worm-like toolkit used in the recent ScreenConnect attacks against managed service providers (MSPs). It is designed to move from an infected customer device to the computer of an MSP technician, and from there to other managed networks.

How the toolkit works

Attackers first install additional ScreenConnect Access clients that connect to their own servers, keeping access even if the original MSP session ends. A component called RelayTrap then replaces the legitimate ScreenConnect Guest process and waits for a technician to connect. It tries to send a malicious file back to the technician, exploiting CVE-2026-84869, a client-side file-transfer flaw that ConnectWise fixed in version 26.6.5.

Other components try to steal ScreenConnect authentication cookies from browsers, which could let attackers take over the technician's session without credentials or a new MFA prompt. They would then use the technician's permissions to enumerate endpoints and push commands, including through the Shared Toolbox.

What has been observed

Both teams say this worm-like behaviour has not succeeded in the current campaign. Blackpoint reproduced the exploit attempt against a current client and found the fix prevented execution. Huntress saw the console takeover fail in every recovered host log it reviewed.

The broader attacks compromised at least 288 endpoints across 48 organizations, all within 90 minutes. Huntress believes initial access came through RMM+ versions 1.0.31 and 1.0.32, where a blank access key let attackers issue commands without authenticating or completing MFA. ConnectWise disabled five related third-party extensions across about 400 partner environments.

The practical lesson is that the technician's workstation is part of the attack surface, and patching clients matters even where exploitation has not yet been seen.

What to do now

1. Update all ScreenConnect clients to version 26.6.5 or later and confirm the update on technician workstations.
2. Disable the affected third-party extensions, including RMM+ versions 1.0.31 and 1.0.32, and set a non-blank access key if the extension is retained.

3. Hunt for unauthorized ScreenConnect Access client installations on managed endpoints.
4. Review Run Command and Shared Toolbox activity for commands without matching user logins.
5. Avoid interactive ScreenConnect sessions with suspected infected endpoints; investigate them with separate security tools.
6. If you outsource IT to an MSP, ask it to confirm its ScreenConnect exposure and response in writing.