

Third-Party Application Compromise

Cybersecurity Incident

On October 15, 2026, ConnectWise reported that a compromised application credential belonging to ConnectWise Cloud Backup, formerly known as SkyKick, was used to sign in to Microsoft 365 environments that had granted the backup service access. Because the application generally holds broad permissions in a tenant, access of this kind would typically not require any user's password. ConnectWise has since disabled the affected applications and suspended the service. As of this writing, ConnectWise has not disclosed how the credential was exposed, and its investigation remains ongoing.

Sandbox Technologies Response

Upon learning of the incident, Sandbox Technologies disabled the affected application access in the tenants under its stewardship and reviewed the available audit logs against the indicators of compromise provided by the vendor. No evidence of unauthorized authentication to any Sandbox Technologies client environment was found in the logs reviewed. Although this review was conducted against the information available at the time, clients will be apprised should the vendor's investigation produce additional indicators.

Vendor Transition

Although there is no finding of negligence on the part of SkyKick or ConnectWise, Sandbox Technologies has concluded that transitioning its clients to another backup provider is in their best interests. Details regarding the replacement platform and transition process will be disseminated in the next few days.

Recommendation - Identity Threat Detection and Response (ITDR)

Huntress published an advisory on this incident and, according to its report, identified the activity and responded within affected partner environments. While Sandbox Technologies places good-faith reliance on its security vendors, no single control removes the risk presented by a trusted third-party application holding tenant-wide permissions.

For this reason, we are strongly recommending that clients using Microsoft 365 or Google Workspace adopt Identity Threat Detection and Response (ITDR), which is generally designed to detect anomalous identity activity in Cloud environments where antivirus, firewalls, and intrusion prevention are typically not positioned to do so.

If you would like to add ITDR to your environment, please respond to this email stating such and we will contact you to initiate the process.

Chris Harper

Chief Security Officer

Sandbox Technologies, Inc.