

> BACKGROUND REPORT FOR PROFESSIONALS

ConnectWise: a stolen backup key opened at least 162 Microsoft 365 tenants

Your key hangs on your provider's key ring

Event: 15 October 2026

Research closed: 23 October 2026 (research revision: v3)

First published: 21 October 2026 · Updated: 23 October 2026

Made with the AI crew, reviewed by Péter

English version of the Hungarian original

Summary

On 15 October 2026, attackers used a stolen vendor credential of the ConnectWise Cloud Backup (formerly SkyKick) Microsoft 365 backup application to sign in to customer tenants, without any user login or MFA: unauthorised sign-in is confirmed in at least 162 tenants, and according to Microsoft more than 2,250 tenants were targeted. On 21 October Microsoft attributed the attack to Storm-0940, a group aligned with Chinese state interests, which used ARTEX, an open-source agentic AI attack framework; in the wider campaign, in several cases less than three hours passed from targeting to privileged access. On 21 October ConnectWise began a phased restoration of the backup service, but full recovery will take several days, and there are no reconnection instructions yet. The most important actions: keep the affected applications disabled until the formal instructions arrive, preserve the evidence, review machine sign-ins and spare keys back to 1 October, and set up a temporary backup.

KEY FINDINGS

- The attack used the backup software vendor's key, not a user account, so MFA offered no protection at all.
- According to Microsoft, the attacker is Storm-0940, a group aligned with Chinese state interests, which targeted more than 2,250 tenants at machine speed using AI agents (ARTEX); this is Microsoft's assessment.
- Sign-in is confirmed in at least 162 tenants; where the attacker got further, it obtained administrator rights and spare keys, which disabling does not reverse.
- On 21 October ConnectWise began a phased restoration of the backup service, but the applications may only be re-enabled after the formal, per-service instructions.

- The extent of data exfiltration and how the key was obtained are still open; Hungarian exposure is not known.

What happened

ConnectWise's **Cloud Backup for Microsoft 365** service (formerly SkyKick Cloud Backup; ConnectWise acquired SkyKick in September 2024) is installed as a Microsoft Entra application – a "machine identity" – in every Microsoft 365 tenant it backs up. This application's credential (a client credential stored in the vendor's own tenant) fell into the wrong hands. On 15 October 2026, the attackers used this key to request Microsoft Graph tokens in customer tenants without any user sign-in – in other words, they signed in as the backup software. **[confirmed: [Huntress](#), [ConnectWise status page](#), [Microsoft according to BleepingComputer](#)]**

The key facts:

- **Perpetrator (new, 2026-10-23):** according to Microsoft's analysis of 21 October 2026, the attack was carried out by **Storm-0940**, which the company tracks as a "China-state aligned" group; it has been active since 2021, and its main goal is data theft. Microsoft bases the attribution in part on the IP addresses published by ConnectWise matching the infrastructure seen in its own investigation. This is Microsoft's assessment ("assesses"), without a formal confidence level; the ConnectWise status page does not comment on the attribution. (*earlier: "no one has named a perpetrator"; updated: 2026-10-23*) **[confirmed as Microsoft's assessment: [Microsoft Security Blog \(primary\)](#); reproduced by: [The Record](#), [The Hacker News](#), [Infosecurity Magazine](#)]**
- **AI agents (new, 2026-10-23):** according to Microsoft, the group used **ARTEX**, an open-source, multi-agent, AI-based penetration testing framework, to speed up reconnaissance, password spraying and the abuse of OAuth applications. The agents can work without human intervention, along several paths at once; according to Microsoft, in the wider campaign running since September, in several cases **less than three hours** passed from targeting to obtaining privileged cloud access. After the abuse became public, the developer made the framework closed source. **[confirmed: Microsoft; The Record; Zscaler ThreatLabz (description of ARTEX)]**
- **Scale:** on 16 October at 19:00 UTC, Huntress confirmed unauthorised sign-ins in **162** tenants; a The Hacker News article of 17 October already speaks of **173** partner and customer tenants. **[reported; the two figures differ, see below]** According to Huntress, there were sign-in attempts from the attacker's address in close to **1,000** Entra tenants, **more than 300** of them successful. According to its 19 October update, Huntress had reviewed the application sign-ins of **more than 10,000** tenants using ConnectWise applications: the applications signed in only from the main attacker address and from Microsoft-internal ranges, and the last confirmed successful attacker sign-in was on 15 October at 08:44 UTC. (*updated: 2026-10-20*) According to Microsoft's own, wider visibility, after obtaining the ConnectWise access the group tried to sign in to **more than 2,250 tenants**, at peak with about 2,900 attempts per minute; most of the attempts failed, but at "many organisations" it gained persistent, privileged cloud access. Microsoft did not give an exact number of successful intrusions. (*updated: 2026-10-23*) **[confirmed: [Huntress](#), [The Hacker News](#), [20 Oct](#); earlier: [Huntress](#); reproduced by: [The Hacker News](#), [iNews](#)]**
- **Permissions:** the permissions previously granted to the backup application gave read and write access to mail (including full mailbox access via EWS), OneDrive and SharePoint files and Teams chats, plus restore rights. Application-level access does not apply to one user but to the whole tenant. **[confirmed: [Todyl](#)]**
- **Privilege escalation:** another ConnectWise application (Cloud Management – MS Teams) made itself Global Administrator in **two** partner tenants (in both around 03:45 UTC on 15 October; earlier: "at least one"; updated: 2026-10-20), and added new secrets to two other trusted applications (an MSP

management tool and Huntress's own application), valid until 2028. This can provide a way back in (a back door) even after the main key is revoked. In about 50 tenants, Cloud Management applications assigned roles to themselves, mostly Exchange Administrator. **[confirmed: Huntress; Microsoft assessment according to BleepingComputer]**

- **What did they do inside? (new, 2026-10-20)** In the two compromised tenants, Huntress **found no mailbox or file modifications and no user or policy changes**; the access was probably used for Microsoft Graph directory reads, which however **leave no audit trail**. This does not mean no data was read: the backup application's read rights made it possible, and reads cannot always be ruled out from the logs. **[confirmed: Huntress (primary), The Hacker News, 20 Oct]**
- **MFA did not protect:** because an application signed in, not a user, there was no password, device or multi-factor confirmation that could have stopped it. **[confirmed: SpecterOps, Todyl]**
- **Second, targeted wave:** in the morning and afternoon of 15 October, the attacker also tried to reach 16 tenants working in policy, national security, trade and critical raw materials; most of them did not even use ConnectWise products, so the attempts largely failed. **[confirmed: Huntress; reproduced by: iTnews, The Hacker News]**
- **Vendor actions:** ConnectWise revoked the affected certificates, invalidated the shared Cloud Backup credentials, according to its 19 October statement restored accounts and **replaced the applications' credentials**, strengthened the protection of administrative access, blocked new sign-ins to its applications, disabled seven application identities on 17 October at 07:00 UTC, brought in an external incident response firm, and as a precaution also took SaaS Security and Cloud Management offline. **[confirmed: ConnectWise status page]**
- **Status (22 October 2026):** on 21 October at 14:35 UTC, ConnectWise announced that it had **begun a phased restoration of the services, subject to security checks**; this does not mean that every function is available, full recovery will take "several days", and it promises per-service reconnection instructions. From 22 October it posts a status update twice a day. (*earlier: on 20 October suspended with no restoration date; updated: 2026-10-23*) **[confirmed: ConnectWise status page (21 Oct, 14:35 and 22 Oct, 00:52 UTC), Infosecurity Magazine, The Hacker News]** Background: Cloud Backup had been suspended since 17 October, SaaS Security and Cloud Management since 18 October; scheduled backups, archive access and restore were unavailable during this time. According to the vendor, it has seen no successful attacker activity in the monitored environments since 17 October, 05:00 UTC, and no other product is affected. Partners should **not re-enable** the affected applications until formal restoration instructions arrive. (*earlier: status of 19 October, 01:28 UTC; updated: 2026-10-20*) **[confirmed: ConnectWise status page (19 Oct, 14:21 UTC), The Hacker News, 20 Oct, ITPro, 20 Oct]**
- **ConnectWise's position:** there is no sign that partners' *backup archives* were accessed; the archives are encrypted and isolated. However, the vendor has no visibility into customer tenants, so it cannot say what happened at a given customer. **[confirmed: ConnectWise; iTnews]**
- **Open:** how the key was obtained, and whether a product flaw played a role. Microsoft's analysis does not describe the initial access either (only that the group typically gets in through password spraying and the exploitation of internet-facing applications), and ConnectWise is investigating with independent experts "how the initial unauthorised access occurred". According to Microsoft, the incident did not stem from a vulnerability in its own systems. (*earlier: "no one has named a perpetrator"; updated: 2026-10-23*) **[confirmed: Microsoft, ConnectWise status page; The Next Web]**

Timeline

Date (UTC)	Event	Source
Sept 2024	ConnectWise acquires SkyKick (and Axcient)	Blumira – reported
Early Sept 2026	Earliest ARTEX-driven Storm-0940 activity observed by Microsoft; the campaign targets hundreds of organisations worldwide	Microsoft – confirmed (Microsoft's assessment)
10–14 Oct 2026	Automated, cross-tenant password spraying: 327 accounts at 8 organisations, 151,000+ failed sign-ins, peaking on 11 Oct (111,000+ that day); no successful sign-in	Microsoft; The Hacker News – confirmed
13–14 Oct 2026	Password-spraying attempts against the tenants of four law firms from the same hosting address; two accounts locked out, no successful user sign-in	Huntress – confirmed
14 Oct 2026	According to The Hacker News, ConnectWise identified the problem on this day	The Hacker News – reported
15 Oct 2026, from 01:58	Cloud Management applications assign roles to themselves in about 50 tenants	Huntress – confirmed
15 Oct 2026, 03:44–03:49	In one tenant the Teams Cloud Management application becomes Global Administrator and adds secrets to two other applications (in about five minutes)	Huntress – confirmed
15 Oct 2026, 06:13–08:34	Scripted token requests in the name of the Cloud Backup application, tenant by tenant, in sorted order, seconds to minutes apart	Huntress; Todyl (07:11–08:47 at its own customers) – confirmed
15 Oct 2026, 09:25–14:20	Targeted second wave against 16 tenants; the afternoon phase appeared to be hands-on	Huntress – confirmed
16 Oct 2026	Huntress raises the alarm; 162 confirmed tenants at 19:00	Huntress, iNews – confirmed
16 Oct 2026, 17:48	ConnectWise: "investigation in progress", containment measures in place	ConnectWise status page – confirmed
17 Oct 2026, 05:11	ConnectWise confirms unauthorised access to application identities and cuts Cloud Backup access	ConnectWise status page – confirmed
17 Oct 2026, 07:00	Seven application identities disabled	ConnectWise status page – confirmed
17 Oct 2026	Microsoft publicly calls it an "active supply chain attack"; 173 tenants in the press	BleepingComputer, The Hacker News – reported
18 Oct 2026	SaaS Security and Cloud Management also offline; further indicators published, remediation guidance for partners	ConnectWise status page – confirmed
18 Oct 2026	A few failed user sign-ins from a new address in the same hosting range	Huntress, The Hacker News – confirmed
19 Oct 2026, 01:28	Services still suspended, no restoration time; partners should keep the applications disabled	ConnectWise status page – confirmed
19 Oct 2026	ConnectWise: accounts restored, application credentials replaced, external incident responders engaged; no successful attacker activity since 17 Oct, 05:00	The Hacker News , 20 Oct , ConnectWise status page – confirmed
19 Oct 2026, 17:30 (13:30 ET)	Huntress update: 10,000+ tenants reviewed, a second compromised tenant, no mailbox or file changes; last confirmed successful attacker sign-in 15 Oct, 08:44	Huntress – confirmed
20 Oct 2026	Services still down, no restoration time	ITPro , 20 Oct , The Hacker News , 20 Oct – confirmed

Date (UTC)	Event	Source
20 Oct 2026, 13:01 and 19:05	ConnectWise: partner webinars every two hours; preparing a phased restoration, "several days"	ConnectWise status page – confirmed
21 Oct 2026	Microsoft attributes the attack to Storm-0940, using the ARTEX AI framework; 2,250+ targeted tenants	Microsoft; The Record; The Hacker News – confirmed (Microsoft's assessment)
21 Oct 2026, 14:35	ConnectWise: phased restoration of the services has begun, subject to security checks	ConnectWise status page; Infosecurity Magazine – confirmed
22 Oct 2026	Restoration in progress, two status updates a day; no per-service reconnection instructions yet	ConnectWise status page – confirmed

Actors and background

- **ConnectWise:** US software vendor building remote management, ticketing, backup and security tools specifically for managed service providers (MSPs, i.e. outsourced IT administration companies). An MSP manages dozens or hundreds of customers from a single ConnectWise console. The company's products have been targeted before, for example through the February 2024 vulnerability in the ScreenConnect remote access software (CVE-2024-1709). **[confirmed: ConnectWise Trust Center]**
- **SkyKick:** Microsoft 365 migration and backup provider, mainly for MSPs; part of ConnectWise since 2024. In older tenants the applications may still appear under the "SkyKick" name. **[confirmed: BleepingComputer, Blumira]**
- **Huntress:** a company providing security monitoring for MSPs; it spotted the attack and published the most detailed analysis. It is also affected itself: in one tenant the attacker added a key to Huntress's application, which the company removed. **[confirmed: Huntress]**
- **Microsoft:** based on its own telemetry, it confirmed widespread application authentication from the suspicious IP and classified the case as a supply chain attack. **[reported: BleepingComputer, The Hacker News]**
- **Sophos X-Ops (new source, 2026-10-20):** saw the same scripted sweep in its own telemetry (15 October, 07:11–08:47 UTC, from a single VPS), and observed that the attacker also went through tenants without an active backup subscription – so it probably used the list of every tenant that had ever consented to the application. **[confirmed: Sophos X-Ops]**
- **Todyl, SpecterOps, Blumira, Coalition:** independent security companies and a cyber insurer that analysed the case across their own customer bases and published verification guidance.
- **Perpetrator – Storm-0940 (updated: 2026-10-23):** a group aligned with Chinese state interests, tracked by Microsoft since 2021 and first described in detail by the company in November 2024; its typical methods are password spraying, exploiting internet-facing applications, and persistence through new credentials added to existing OAuth applications. According to Microsoft, its targets include the defence and aerospace industries, energy, financial services, government, the legal sector, the semiconductor industry and think tanks. *(earlier: "unknown")* **[confirmed as Microsoft's assessment: Microsoft; Infosecurity Magazine; The Hacker News]**
- **ARTEX:** a multi-agent AI penetration testing framework written in Go, released as open source on GitHub in early 2026, which works with any language model; the agents can carry a test through on their own, from reconnaissance to data exfiltration. It was originally built for authorised testing; on 8 October the developer announced that it had been abused and made the project closed source. On 14 October Zscaler described its use in a financially motivated campaign against South Korean

financial institutions; according to Microsoft, several groups in several regions use it. **[confirmed: Microsoft, Zscaler ThreatLabz, The Record]**

- **China's reaction:** citing Reuters, The Record writes that a spokesperson for the Chinese foreign ministry denied any knowledge of the incidents; the article does not make clear whether this referred to the ConnectWise attribution or to the earlier ARTEX-related cases. **[reported: The Record]**

Precedents: not the first "one key, many doors" case

- **Kaseya VSA, 2 July 2021:** the REvil ransomware group used zero-day flaws in Kaseya's on-premises remote management software to encrypt 800–1,500 end customers via about 50–60 MSPs. Same pattern: the MSP's tool gives access to many companies through a single point. **[confirmed: TechTarget]**
- **Midnight Blizzard at Microsoft, January 2024:** a Russian state group took over a forgotten but highly privileged OAuth application from an old test tenant without MFA, and used it to reach mailboxes. Same lesson: machine identities and old application permissions often fall outside the field of view. **[confirmed: Microsoft]**
- **Salesloft Drift, August 2025:** the group tracked as UNC6395 used stolen OAuth tokens of a chatbot integration to download the Salesforce data of numerous companies. Google advised treating every token connected to Drift as compromised. **[confirmed: Google GTIG according to Security Affairs]**
- **Trend:** attackers increasingly target not passwords but the "machine trust" between services (OAuth applications, API keys, tokens), because MFA does not help there and logging is weaker. **[assumption, based on the three cases above and the SpecterOps analysis]**

How it works

RED // ATTACKER'S VIEW

Conceptually, why it could work:

1. **The key is with the vendor, not with you.** When an MSP turns on cloud backup, the Microsoft 365 administrator approves once ("consent") that the backup application may read all mail and files. From then on, the application can request a token at any time with the vendor's own key. According to Huntress, nothing the customer did in its own environment could have produced this credential. **[confirmed: Huntress]**
2. **One key for every lock.** A multi-tenant application has one identity that works in every tenant where it was approved. Whoever obtains it can go through every customer on a list; according to the logs, this is exactly what the attacker did, automatically and in sorted order. **[confirmed: Huntress, Todyl]**
3. **No human, no MFA.** A machine signs in to a machine, so protections built for users (MFA, risky sign-in detection, device compliance) do not apply. Conditional Access can be applied only to a limited extent to external multi-tenant applications. **[confirmed: SpecterOps, Todyl, Blumira]**
4. **Malicious traffic looks like normal backup.** A backup tool's job is to read mail and files in bulk. The attacker can do the same with the same identity, so according to Todyl, in tenants with active backup it was impossible to separate legitimate from malicious reads. **[confirmed: Todyl, Coalition]**
5. **The logs are incomplete.** Directory reads via Graph do not always leave an audit trail, the audit log does not record the source IP for application-level operations, free Entra ID keeps logs for only 7 days, and the detailed Graph activity log must be enabled separately (P1/P2 licence) and is not retroactive. **[confirmed: Huntress, Todyl, Blumira]**
6. **Persistence through other applications.** If a trusted application gets an administrator role, it can add new secrets to other applications. That way the attacker can come back even if the original key is

revoked – which is why disabling only the ConnectWise application is not enough. **[confirmed: Huntress, SpecterOps]**

7. **Disabling is not instant.** Tokens already issued remain valid for up to about 60–90 minutes after disabling. Revoking user sessions has no effect on them. **[confirmed: Todyl, Blumira]**

8. **Machine speed (new, 2026-10-23).** According to Microsoft, the attacker used AI agents that do not get tired, work day and night, and try several intrusion paths at once. This does not mean a new technique, but the acceleration of existing ones (reconnaissance, password spraying, abuse of application permissions): according to Microsoft, in several cases less than three hours passed from targeting to privileged access, which leaves human defenders hardly any time to react. The lesson: where defence relies on manual alert handling, prevention (narrow permissions, short-lived keys) is worth more than fast detection. **[confirmed: Microsoft; The Record; interpretation: assumption]**

So the weakness is not a classic "hole" but the design of the chain of trust: broad, standing permissions, a single shared key, weak visibility. The Promptly Secured angle sums it up like this: *your key hangs on your provider's key ring.*

Impact and the Hungarian angle

Known impact:

- 162 → 173 confirmed tenants with unauthorised sign-ins; attempts in close to 1,000 tenants, more than 300 successful sign-ins (Huntress, with its visibility beyond ConnectWise). One organisation can run several tenants, so the number of tenants does not equal the number of companies. **[reported: Huntress, tech-insider]**
- According to Microsoft, Storm-0940 used the ConnectWise access to target more than 2,250 tenants; most attempts failed, but at "many organisations" it gained persistent, privileged access, and where it got further, it carried out reconnaissance, added application credentials and modified roles, groups and identities. Microsoft stresses that the presence of an affected application or a successful sign-in does not in itself mean that customer data was accessed or exfiltrated. (*new, 2026-10-23*) **[confirmed: Microsoft; Infosecurity Magazine]**
- Law firms (password spraying) and strategic sectors (second wave) were among the priority targets; the target sectors listed by Microsoft (defence industry, government, energy, finance, legal, semiconductors, think tanks) are consistent with this. **[confirmed: Huntress, Microsoft]**
- The extent of data exfiltration is unknown. In the two compromised tenants it examined, Huntress found no mailbox or file changes, but Graph reads leave no trace (*updated: 2026-10-20*); earlier, some MSPs reported on Reddit that e-mail, Teams and SharePoint data had been copied out, which neither ConnectWise nor Huntress has confirmed. In nine tenants without a backup subscription, Todyl saw only sign-in and reconnaissance, no further activity. **[reported: Blumira, Coalition; confirmed: Todyl]**
- **Side effect: companies left without backup.** Because of the precautions, Cloud Backup customers have not been able to back up or restore since 17 October; the phased restoration began on 21 October, but on 22 October full recovery will still take "several days" (*earlier: on 20 October with no restoration date; updated: 2026-10-23*). Cyber insurer Coalition warns: if another incident (for example ransomware) happens in this window, recovery is harder. **[confirmed: ConnectWise status page; Coalition]**
- **Concentration risk:** according to Coalition, an MSP typically uses one backup vendor for all its customers, so a vendor incident can cause losses for many policyholders at once. **[assumption:**

Coalition]

Hungarian and regional angle:

- **Hungarian exposure is not known.** Searches on 19, 20 and 23 October 2026 found neither a warning from a Hungarian authority (NBSZ NKI, Hungary's national cyber security centre; SZTFH, the regulator supervising most companies under NIS2) nor any Hungarian press article about the case, nor about the Storm-0940 attribution. Microsoft's analysis speaks of "global" targeting and names no country or region; Europe and Hungary do not appear in it. (*updated: 2026-10-23*) None of the sources gave a breakdown by country; iTnews explicitly notes that it knows of no Australian or European figures. **[confirmed absence in the examined sources]**
- Because SkyKick/ConnectWise sells specifically through the MSP channel, and Microsoft 365 is also widespread among Hungarian SMEs, it cannot be ruled out that customers of Hungarian MSPs are affected. **[assumption]**
- **Regulatory angle:** under Hungary's transposition of NIS2, the companies in scope are responsible for the IT security of their supply chain, and according to an expert quoted by Portfolio, outsourcing does not transfer responsibility: "the ultimate responsibility lies with the organisation using the service". The supervisory authority for most companies is the SZTFH. **[reported: Portfolio, in Hungarian]**

What to do

BLUE // WHAT TO DO NOW

Individual (using a company or small-business Microsoft 365)

- Ask your company's IT team or administrator: do we use ConnectWise Cloud Backup or SkyKick, and have the disabling and the checks been done?
- If you have your own business with an MSP: ask them for written feedback on the small-business points below.
- Over the coming weeks, be careful with e-mails that sound familiar but contain an unusual request (for example a change of bank account number, an urgent transfer). If someone had access to the mailbox, they can write convincing fraudulent e-mails from it. When in doubt, call the sender on a known number. **[assumption, general precaution]**

Small business (Microsoft 365 tenant, with an external IT partner)

- Ask your MSP to search your tenant for all ConnectWise and SkyKick applications, *even if you stopped using them long ago*, and to disable them (disable, not delete) until ConnectWise confirms that the keys have been replaced. **[Huntress, Todyl, Blumira]**
- Before disabling, export the application's permission list and the logs: free Entra ID keeps logs for only 7 days. **[Todyl, Blumira, Coalition]**
- Ask: did these applications get an administrator role, and has a new secret or certificate been added to any application since 13 October 2026? **[Huntress]**
- Make sure you have a temporary backup (the phased restoration started on 21 October, but full recovery will take "several days"; updated: 2026-10-23): while Cloud Backup is down, have at least one other recent backup of critical mailboxes and files. **[based on Coalition, ConnectWise status page]**

- If you have cyber insurance, check whether you need to report the suspicious activity, and preserve the logs. **[Coalition]**
- In the longer term, ask your MSP: which external applications have you given tenant-wide rights in my name, and which of them are actually needed? Ask for this every year, in writing.

Organisation (with in-house IT, or as an MSP)

- **Immediately:** disable the Cloud Backup application and the Teams Cloud Management application in every tenant; also the other ConnectWise/SkyKick Cloud Management applications, until the vendor issues formal restoration instructions. **[Huntress, ConnectWise]**
- **Log review:** on the Entra "Service principal sign-ins" tab (not the user sign-ins!), filter for the application ID and look for authentication from ranges other than Microsoft/Azure; back to 1 October, or as far as retention allows. **[Huntress, Todyl, ConnectWise]**
- **Audit log:** role assignments, consents and new credentials on every application since 13 October, with particular attention to management and security tools. Revoke Global Administrator and Privileged Authentication Administrator roles that were not granted intentionally. **[Huntress]**
- **Unified audit log:** mail, file and Teams read events where the client application is the affected application; unusual bulk reads outside the backup schedule; new mailbox rules and permissions. **[Todyl, Coalition, Blumira]**
- **Do not re-enable too early (new, 2026-10-20):** re-enable the affected applications only after ConnectWise's formal restoration instructions; according to the vendor, disabling only prevents new connections and does not reverse changes made earlier in the tenant. Do the review from 13 October, but preferably from 1 October, including long-unused ("dormant") SkyKick connections. **[ConnectWise according to ITPro, 20 Oct and The Hacker News, 20 Oct; Infosecurity Magazine]**
- **Microsoft's investigation recommendations (new, 2026-10-23):**
 - Do not delete the affected enterprise applications as a first step: first preserve the configuration and the evidence (Entra sign-in and audit logs, Purview audit, SIEM, Graph telemetry), but do not delay disabling while waiting for the export.
 - Search for the applications by application ID, not by display name, and record the local service principal object ID for each tenant.
 - Review every tenant where the application was ever installed or consented to, even if it is not in use.
 - Examine successful and failed service principal sign-ins separately, at least from 15 October, and for service principal sign-ins back to 1 October; do not filter only for the published IP addresses, but for every source outside the vendor's usual infrastructure.
 - In the audit log, look for: new credentials, new applications, service principals or owners, app role assignments, consents, privileged role changes, and changes to users, groups, authentication methods and Conditional Access.
 - If you use Azure Key Vault, also look for unusual bulk secret reads.
 - After the evidence has been preserved, an authorised incident responder should remove the confirmed unauthorised credentials, consents, owners and assignments, and rotate keys wherever there was suspicious activity.
 - Verify that the vendor's key rotation and the tenant-level remediation have actually eliminated all unauthorised access. **[confirmed: Microsoft]**
- **When reconnecting (new, 2026-10-23):** re-enable the applications only on the basis of ConnectWise's formal, per-service instructions; on 22 October no such instructions had been issued yet. Have the review above completed before reconnecting. **[ConnectWise status page, Microsoft]**

- **Visibility:** turn on the Microsoft Graph activity log (not retroactive), and increase log retention. [Huntress, Todyl]
- **Hardening:** use app management policies to restrict the use and lifetime of secrets; narrow the scope of the Application Administrator and Cloud Application Administrator roles; where the licence allows, use Conditional Access and Entra ID Protection for workload identities; in Exchange, use application RBAC to restrict which mailboxes an application can access. [Huntress, Microsoft]
- **Third-party risk (TPRM):** keep a register of every multi-tenant application, its permissions and its owner; in the MSP contract, specify incident notification, access restriction, logging and revocation of access at the end of the contract. [Joint ASD/CISA/NCSC guidance: cyber.gov.au; Portfolio]
- **Exiting a provider:** cancelling the subscription does not end the vendor's access; the application consent has to be revoked separately. [Blumira]

Technical block

- **CVE:** none. As currently known, this is a credential compromise, not a published vulnerability; according to ConnectWise, it is not yet known whether a product flaw contributed. [The Hacker News]
- **Affected components:** the ConnectWise Cloud Backup (SkyKick) Microsoft 365 enterprise application, and the Cloud Management application family (MS Teams, Exchange Online, MS Graph, Partner Center, SharePoint Online). ConnectWise disabled seven application identities in total. In older tenants they may also appear under the name "SkyKick Cloud Manager". [ConnectWise, BleepingComputer]
- **Authentication flow:** OAuth 2.0 client credentials (application-level, app-only token), with clientAssertion-type authentication, using a key stored in the vendor tenant. [Huntress, Todyl]
- **Permissions abused:** according to Microsoft, probably Directory.ReadWrite.All; according to Todyl, mail, file and Teams read/write, and full mailbox access via EWS. [BleepingComputer, Todyl]
- **MITRE ATT&CK (according to Huntress):**
 - T1078.004 – Valid Accounts: Cloud Accounts (use of the vendor key)
 - T1098.003 – Account Manipulation: Additional Cloud Roles (self-assigned Global and Exchange Administrator)
 - T1098.001 – Account Manipulation: Additional Cloud Credentials (secrets on other applications)
 - In addition: T1110.003 Password Spraying (13–14 October) [based on the described behaviour: assumption]
 - In addition, according to Microsoft's analysis of 21 October (updated: 2026-10-23): T1595 Active Scanning; T1195 Supply Chain Compromise; T1199 Trusted Relationship (*earlier: assumption; now also listed by Microsoft*); T1528 Steal Application Access Token; T1555.006 Cloud Secrets Management Stores (bulk Key Vault secret reads); T1087.004 Cloud Account; T1580 Cloud Infrastructure Discovery. [confirmed: Microsoft]
- **Microsoft Defender detections (conceptual):** an application that assigned itself the Global Administrator role; sign-in from known attacker or confirmed state-actor infrastructure; suspicious app role assignment to a service principal; Key Vault access anomaly. Microsoft has also published advanced hunting and Sentinel queries. [confirmed: Microsoft]
- **Detection ideas (conceptual):**
 - Service principal sign-ins where the source is not the vendor's usual (Azure private IPv6) egress but a public hosting provider.
 - An application that assigns itself a role, or adds a credential to another application.

- The combination of user agent and operation: ConnectWise's own applications run with a different agent than the attacker scripts; neither agent alone is a reliable signal. **[Huntress]**
- Graph-based analysis (e.g. BloodHound/AzureHound) to map paths from external applications to the most privileged (Tier Zero) resources. **[SpecterOps]**
- **Indicator types and official sources:** IP addresses (from one hosting provider's range; ConnectWise published more on 18 October, and on 21 October Microsoft also published transient VPN addresses), application IDs, vendor tenant ID, user agents, session ID pattern. Full list: [Microsoft](#), [Huntress](#), [Todyl](#), [ConnectWise status page](#). Important: the Cloud Backup application ID is *legitimate* and must not be blocklisted – only disable the application. **[Huntress]**
- **Official recommendations:** ConnectWise remediation guidance for partners (linked on the status page), Huntress, Todyl and SpecterOps guidance; as background, Microsoft's Midnight Blizzard guidance against OAuth application abuse, and the joint ASD/CISA/NCSC/NSA/FBI MSP advisory.

Contradictions and open questions

Open questions

- **162 or 173?** The Huntress blog says 162 (16 October, 19:00 UTC); The Hacker News and several secondary sites say 173 (17 October), attributing it to Huntress, but 173 still does not appear in the Huntress blog on 23 October. On 21 October Microsoft published a third figure of a different kind: 2,250+ *targeted* tenants. In summary: "sign-in is confirmed in at least 162 tenants; according to Microsoft, more than 2,250 tenants were targeted". (*updated: 2026-10-23*)
- **When did ConnectWise know?** According to the sources, on 14 October (The Hacker News), on 15 October (Infosecurity Magazine, SecurityWeek), or on 16 October (ITPro); the first status page entry is 16 October, 17:48 UTC. Still cannot be decided. What can be said for certain: "the vendor informed the public on 16 October".
- **Were all of them disabled? Closed (2026-10-20):** it was a timing difference; according to Huntress's update of 17 October, ConnectWise had by then confirmed the disabling.
- **The time window:** Huntress 06:13–08:34, Todyl and Sophos 07:11–08:47 UTC (different customer bases) – not a contradiction; in summary: "early morning (UTC) of 15 October".
- **"The backed-up data was not affected" – but what about the live data?** ConnectWise spoke about the *archives*, and on 21–22 October it again stressed that this says nothing about the state of individual customer tenants. Microsoft likewise says that a successful sign-in does not automatically mean that data was accessed or exfiltrated.
- **Who and why? Partly closed (2026-10-23):** Microsoft attributes it to Storm-0940, which according to the company typically seeks data theft. This is a single company's assessment, without a formal confidence level; the ConnectWise status page does not comment on it, and the press describes the vendor's reaction differently (The Next Web: did not respond; Infosecurity Magazine: issued an update acknowledging Microsoft's findings). Promptly Secured therefore words it as: "according to Microsoft, a group aligned with Chinese state interests".
- **What does the "three hours" refer to?** Microsoft writes about the wider ARTEX campaign running since September that in several cases less than three hours passed from targeting to privileged access; the text does not make clear whether this also applies specifically to ConnectWise customer tenants. We therefore report it as applying to the campaign. (*new, 2026-10-23*)
- **How much did AI matter?** Reconnaissance, password spraying and the abuse of application permissions are known techniques; according to Microsoft, the AI agents added speed and

parallelism. Microsoft did not say which model was used, and the examined sources contain no independent expert assessment of the role of AI. (new, 2026-10-23)

- **How did the key get out?** Still not known; ConnectWise is investigating with independent experts, and Microsoft does not describe it either.
- **Was data exfiltrated?** Still not known; there are no changes in the two tenants Huntress examined, and where the attackers got further, Microsoft saw reconnaissance and permission changes, but did not confirm data exfiltration in this campaign.
- **When will backups fully return, and what will the reconnection instructions be?** The phased restoration started on 21 October; there were no per-service instructions yet on 22 October.

Source assessment

Source	Type	Reliability	What it supports
Huntress blog	researcher (primary)	high	timeline, 162 tenants, techniques, ATT&CK, second wave, recommendations, IOCs
ConnectWise status page	company (primary)	high (on its own statements)	vendor actions, service status, state of the archives
Todyl	researcher (primary)	high	permissions, token lifetime, analysis of 9 tenants, detection
SpecterOps	researcher	high	explanation of the MFA bypass, attack paths, verification
BleepingComputer	press	high	Microsoft assessment, timeline, ConnectWise statements
The Hacker News – 173 tenants	press	medium–high	the figure of 173, summary
The Hacker News – suspension	press	medium–high	~1,000/300 tenants, identification on 14 Oct, disabling contradiction
iNews	press	high	ConnectWise statement of 19 Oct, lack of regional data
Coalition	company (insurer)	medium–high	insurance and concentration risk, recovery impact
Blumira	company (security vendor)	medium	SME-specific risks, log retention, MSP reports
tech-insider	press (secondary)	low–medium	origin of the figure 173 (contested)
Microsoft – Midnight Blizzard	company (primary)	high	precedent, OAuth defence
Security Affairs – Salesloft Drift	press	medium–high	precedent (2025)
TechTarget – Kaseya	press	high	precedent (2021)
cyber.gov.au – MSP advisory	authority	high	actions for MSP customers
The Hacker News – credential reset (20 Oct)	press	medium–high	vendor remediation of 19 Oct, Huntress 10,000+ tenants, new IPs
ITPro (20 Oct)	press	high	status on day three, "disabling does not reverse", review back to 1 Oct
Sophos X-Ops	researcher (primary)	high	independent confirmation, tenants without subscription also on the list
SecurityWeek	press	high	order of service shutdowns, CoreView quote

Source	Type	Reliability	What it supports
Infosecurity Magazine	press	high	ConnectWise recommendations, absence of attribution
Portfolio – NIS2 (HU)	press (HU)	medium	NIS2 supply chain, SZTFH
Microsoft Security Blog – Storm-0940/ARTEX (21 Oct)	company (primary)	high (on its own assessment)	attribution, ARTEX use, 2,250+ tenants, timeline, investigation recommendations, ATT&CK, IOCs
The Record (22 Oct)	press	high	reproduction of the attribution, ARTEX developer's statement, Chinese denial
The Hacker News – ARTEX (22 Oct)	press	medium–high	Storm-0940 background, password-spraying figures, phased restoration
Infosecurity Magazine – Microsoft attribution	press	high	target sectors, ConnectWise statements, restoration
Zscaler ThreatLabz (14 Oct)	researcher (primary)	high	description of ARTEX; the South Korean campaign (not the ConnectWise case)
The Next Web (22 Oct)	press	medium	summary, lack of ConnectWise reaction, Microsoft: not its own vulnerability

Changelog

- 20 October 2026 (v2):** The services have been down since 17 October, and ConnectWise has replaced the credentials; after reviewing 10,000+ tenants, Huntress found a second compromised tenant, but no mailbox or file changes. The timeline and the actions were extended (do not re-enable too early, temporary backup), and a follow-up article angle was added.
- 23 October 2026 (v3):** On 21 October Microsoft attributed the attack to Storm-0940, a group aligned with Chinese state interests, which used the ARTEX agentic AI framework (2,250+ targeted tenants); Microsoft's investigation recommendations, the extended ATT&CK list, and the fact that ConnectWise began a phased restoration on 21 October were added. New follow-up angle: intrusion at machine speed.