

> HÁTTÉRANYAG SZAKMABELIEKNEK

ConnectWise: ellopott mentési kulccsal léptek be legalább 162 Microsoft 365-bérlőbe

A te kulcsod a szolgáltatód kulcskarikáján lóg

Esemény: 2026. október 15.

Lezárva: 2026. október 23. (kutatási változat: v3)

Első kiadás: 2026. október 21. • Frissítve: 2026. október 23.

AI-csapattal készült, átnézte: Péter

Összefoglaló

2026. október 15-én támadók a ConnectWise Cloud Backup (korábban SkyKick) Microsoft 365-mentőalkalmazás ellopott gyártói hitelesítő adatával, felhasználói belépés és MFA nélkül jelentkeztek be ügyfélbérlőkbe: legalább 162 bérlőben igazolt a jogosulatlan belépés, a Microsoft szerint több mint 2250 bérlőt próbáltak elérni. A Microsoft október 21-én a támadást a kínai állami érdekekhez igazodó Storm-0940 csoportnak tulajdonította, amely az ARTEX nevű, nyílt forrású AI-ügynökös támadókeretet használta; a tágabb kampányban több esetben három óránál rövidebb idő telt el a célba vételtől a kiemelt jogosultságig. A ConnectWise október 21-én szakaszosan elkezdte visszaállítani a mentést, de a teljes helyreállítás több napig tart, és újrapcsolási utasítás még nincs. A legfontosabb teendő: az érintett alkalmazások letiltva tartása a formális utasításig, a bizonyítékok mentése, a gépi bejelentkezések és a pótkulcsok átnézése október 1-ig visszamenőleg, és ideiglenes mentés.

KULCSMEGÁLLAPÍTÁSOK

- A támadás nem felhasználói fiókot, hanem a mentőszoftver gyártói kulcsát használta, ezért az MFA egyáltalán nem védett.
- A Microsoft szerint a támadó a kínai állami érdekekhez igazodó Storm-0940, amely AI-ügynökökkel (ARTEX) gépi sebességgel, több mint 2250 bérlőt célzott meg; ez a Microsoft értékelése.
- Legalább 162 bérlőben igazolt a belépés; ahol a támadó továbbjutott, rendszergazdai jogot és pótkulcsokat szerzett, amit a letiltás nem fordít vissza.
- A ConnectWise október 21-én szakaszosan elkezdte visszaállítani a mentést, de az alkalmazásokat csak a szolgáltatásonkénti formális utasítás után szabad visszakapcsolni.

- Az adatkiszivárgás mértéke és a kulcs megszerzésének módja továbbra is nyitott; magyar érintettség nem ismert.

Mi történt

A ConnectWise **Cloud Backup for Microsoft 365** szolgáltatása (korábbi nevén SkyKick Cloud Backup; a ConnectWise 2024 szeptemberében vásárolta meg a SkyKicket) egy Microsoft Entra-alkalmazásként, azaz „gépi identitásként” van telepítve minden olyan Microsoft 365-bérlőben (tenantban), amelyet ment. Ennek az alkalmazásnak a hitelesítő adata (egy, a gyártó saját bérlőjében tárolt kliens-hitelesítés) illetéktelen kézbe került. A támadók 2026. október 15-én ezzel a kulccsal, felhasználói bejelentkezés nélkül kértek Microsoft Graph tokeneket az ügyfélbérlőkben, vagyis a mentőszoftver nevében léptek be. **[megerősített: [Huntress](#), [ConnectWise státuszoldal](#), Microsoft a [BleepingComputer](#) szerint]**

A legfontosabb tények:

- **Elkövető (új, 2026-10-23):** a Microsoft 2026. október 21-i elemzése szerint a támadásért a **Storm-0940** felelős, amelyet a cég kínai állami érdekekhez igazodó („China-state aligned”) csoportként követ; 2021 óta aktív, fő célja az adatlopás. A Microsoft a hozzárendelést részben arra alapozza, hogy a ConnectWise által közölt IP-címek egyeztek a saját vizsgálatában látott infrastruktúrával. Ez a Microsoft értékelése („assesses”), formális bizonyossági szint nélkül; a ConnectWise státuszoldala a hozzárendelésről nem nyilatkozik. *(korábban: „elkövetőt senki nem nevezett meg”; frissítve: 2026-10-23)* **[megerősített mint Microsoft-értékelés: [Microsoft Security Blog](#) (elsődleges); átvéve: [The Record](#), [The Hacker News](#), [Infosecurity Magazine](#)]**
- **AI-ügynökök (új, 2026-10-23):** a Microsoft szerint a csoport az **ARTEX** nevű, nyílt forrásként kiadott, többügynökös AI-alapú behatolásteszt-keretrendszert használta a felderítés, a jelszószórás és az OAuth-alkalmazásokkal való visszaélés felgyorsítására. Az ügynökök emberi beavatkozás nélkül, egyszerre több úton haladhatnak; a Microsoft szerint a tágabb, szeptember óta tartó kampányban több esetben **három óránál rövidebb** idő telt el a célba vételtől a kiemelt felhőjogosultság megszerzéséig. A keretrendszert a fejlesztő a visszaélések nyilvánosságra kerülése után zárt forrásúvá tette. **[megerősített: Microsoft; [The Record](#); [Zscaler ThreatLabz](#) (az ARTEX leírása)]**
- **Méret:** a Huntress október 16-án 19:00 UTC-kor **162** bérlőben igazolt jogosulatlan bejelentkezést; a The Hacker News október 17-i cikke már **173** partner- és ügyfélbérlőről ír. **[jelentett, a két szám eltér, lásd lent]** A Huntress szerint közel **1000** Entra-bérlőben volt bejelentkezési kísérlet a támadói címről, ebből **300-nál több sikeres**. Október 19-i frissítése szerint a Huntress már **több mint 10 000**, ConnectWise-alkalmazást használó bérlő alkalmazás-bejelentkezéseit nézte át: alkalmazásként csak a fő támadói címről és Microsoft-belső tartományokból jelentkeztek be, az utolsó igazolt sikeres támadói bejelentkezés október 15-én 08:44 UTC-kor volt. *(frissítve: 2026-10-20)* A Microsoft saját, szélesebb rálátása szerint a csoport a ConnectWise-hozzáférés megszerzése után **több mint 2250 bérlőbe** próbált belépni, csúcson percenként kb. 2900 kísérlettel; a próbálkozások többsége sikertelen volt, de „sok szervezetnél” tartós, kiemelt felhőhozzáférést szerzett. Pontos sikeres darabszámot a Microsoft nem közölt. *(frissítve: 2026-10-23)* **[megerősített: [Huntress](#), [The Hacker News](#), okt. 20.; korábbi: [Huntress](#); átvéve: [The Hacker News](#), [iNews](#)]**
- **Jogosultság:** a mentőalkalmazás korábban megadott engedélyei olvasási és írási hozzáférést adtak a levelezéshez (teljes postafiók-hozzáférés EWS-en keresztül is), a OneDrive- és SharePoint-fájlokhoz, a Teams-csevegésekhez, valamint visszaállítási jogot. Az alkalmazásszintű hozzáférés nem egy felhasználóra szól, hanem a teljes bérlőre. **[megerősített: [Todyl](#)]**
- **Jogosultság-emelés:** egy másik ConnectWise-alkalmazás (Cloud Management – MS Teams) **két** partnerbérlőben is globális rendszergazdává tette magát (mindkettőben október 15-én 03:45 UTC körül; korábban: „legalább egy”; frissítve: 2026-10-20), és új titkos kulcsokat adott két másik

megbízható alkalmazáshoz (egy MSP-felügyeleti eszközhöz és a Huntress saját alkalmazásához), 2028-ig érvényes lejárattal. Ez visszatérési lehetőséget (hátsó ajtót) jelenthet a fő kulcs visszavonása után is. Kb. 50 bérlőben a Cloud Management-alkalmazások szerepkört rendeltek magukhoz, többnyire Exchange-rendszergazdát. **[megerősített: Huntress; Microsoft-értékelés a BleepingComputer szerint]**

- **Mit csináltak bent? (új, 2026-10-20)** A Huntress a két kompromittált bérlőben **nem talált postafiók- vagy fájlmodosítást, felhasználói vagy szabályzatváltozást**; a hozzáférést valószínűleg Microsoft Graph-könyvtárolvasásra használták, ami viszont **nem hagy auditnyomot**. Ez nem jelenti, hogy adatot nem olvastak: a mentőalkalmazás olvasási joga ezt lehetővé tette, és az olvasás a naplókban nem mindig zárható ki. **[megerősített: Huntress (elsődleges), The Hacker News, okt. 20.]**
- **MFA nem védett:** mivel alkalmazás jelentkezett be, nem felhasználó, nem volt jelszó, eszköz vagy többfaktoros megerősítés, amely megállíthatta volna. **[megerősített: SpecterOps, Todyl]**
- **Második, célzott hullám:** október 15-én délelőtt és délután a támadó 16 olyan bérlőt is megpróbált elérni, amelyek a szakpolitika, a nemzetbiztonság, a kereskedelem és a kritikus nyersanyagok területén működnek; ezek többsége nem is használt ConnectWise-terméket, ezért a kísérletek nagyrészt kudarcot vallottak. **[megerősített: Huntress; átvéve: iNews, The Hacker News]**
- **Gyártói lépések:** a ConnectWise visszavonta az érintett tanúsítványokat, érvénytelenítette a megosztott Cloud Backup-hitelesítő adatokat, október 19-i közlése szerint fiókokat állított vissza és **lecserélte az alkalmazások hitelesítő adatait**, megerősítette az adminisztratív hozzáférések védelmét, letiltotta az új bejelentkezéseket az alkalmazásaiba, október 17-én 07:00 UTC-kor hét alkalmazásidentitást letiltott, külső incidenskezelő céget vont be, és óvatosságból a SaaS Security és a Cloud Management szolgáltatást is lekapcsolta. **[megerősített: ConnectWise státuszoldal]**
- **Állapot (2026. október 22.):** a ConnectWise október 21-én 14:35 UTC-kor bejelentette, hogy **szakaszosan, biztonsági ellenőrzéshez kötve megkezdte a szolgáltatások visszaállítását**; ez nem jelenti, hogy minden funkció elérhető, a teljes helyreállítás „több napig” tart, és szolgáltatásonkénti újrapcsolási utasítást ígér. Október 22-től naponta kétszer ad státuszt. *(korábban: október 20-án visszaállítási időpont nélkül szünetelt; frissítve: 2026-10-23)* **[megerősített: ConnectWise státuszoldal (okt. 21., 14:35 és okt. 22., 00:52 UTC), Infosecurity Magazine, The Hacker News]**
Előzmény: a Cloud Backup október 17., a SaaS Security és a Cloud Management október 18. óta szünetelt; ütemezett mentés, archívum-hozzáférés és visszaállítás ez idő alatt nem volt elérhető. A gyártó szerint október 17., 05:00 UTC óta nem látott sikeres támadói aktivitást a figyelt környezetekben, és más terméke nem érintett. A partnerek **ne kapcsolják vissza** az érintett alkalmazásokat, amíg formális visszaállítási utasítás nem jön. *(korábban: október 19., 01:28 UTC-s állapot; frissítve: 2026-10-20)* **[megerősített: ConnectWise státuszoldal (okt. 19., 14:21 UTC), The Hacker News, okt. 20., ITPro, okt. 20.]**
- **A ConnectWise álláspontja:** nincs jele annak, hogy a partnerek *mentési archívumaihoz* hozzáfértek volna; az archívumok titkosítva és elkülönítve vannak. A gyártó ugyanakkor az ügyfélbérlőkbe nem lát bele, így azt nem tudja megmondani, hogy egy adott ügyfélnél mi történt. **[megerősített: ConnectWise; iNews]**
- **Nyitott:** hogyan szerezték meg a kulcsot, és szerepet játszott-e termékhiba. A Microsoft elemzése sem írja le a kezdeti hozzáférést (csak azt, hogy a csoport jellemzően jelszószórással és internetre nyitott alkalmazások kihasználásával jut be), a ConnectWise pedig független szakértőkkel vizsgálja, „hogyan történt az első jogosulatlan hozzáférés”. A Microsoft szerint az incidens nem a saját rendszereinek sebezhetőségéből fakadt. *(korábban: „elkövetőt senki nem nevezett meg”; frissítve: 2026-10-23)* **[megerősített: Microsoft, ConnectWise státuszoldal; The Next Web]**

Idővonal

Dátum (UTC)	Esemény	Forrás
2024. szept.	A ConnectWise felvásárolja a SkyKicket (és az Axcientet)	Blumira – jelentett
2026. szept. eleje	A Microsoft által megfigyelt legkorábbi ARTEX-vezérelt Storm-0940-aktivitás; a kampány több száz szervezetet céloz világszerte	Microsoft – megerősített (Microsoft-értékelés)
2026. okt. 10–14.	Automatizált, bérlőkön átívelő jelszószórás: 8 szervezet 327 fiókja, 151 000+ sikertelen belépés, csúcs okt. 11-én (aznap 111 000+); sikeres belépés nem volt	Microsoft; The Hacker News – megerősített
2026. okt. 13–14.	Jelszószórásos próbálkozás négy ügyvédi iroda bérlője ellen ugyanarról a hosting-címről; két fiók zárolódott, sikeres felhasználói belépés nem volt	Huntress – megerősített
2026. okt. 14.	A ConnectWise a The Hacker News szerint ekkor azonosította a problémát	The Hacker News – jelentett
2026. okt. 15., 01:58-tól	Kb. 50 bérlőben a Cloud Management-alkalmazások szerepkört rendelnek magukhoz	Huntress – megerősített
2026. okt. 15., 03:44–03:49	Egy bérlőben a Teams Cloud Management-alkalmazás globális rendszergazda lesz, és titkos kulcsokat ad két másik alkalmazáshoz (kb. öt perc alatt)	Huntress – megerősített
2026. okt. 15., 06:13–08:34	Szkriptelt tokenkérések a Cloud Backup-alkalmazás nevében, bérlőről bérlőre, rendezett sorrendben, másodpercek-percek különbséggel	Huntress; Todyl (saját ügyfeleinél 07:11–08:47) – megerősített
2026. okt. 15., 09:25–14:20	Célzott második hullám 16 bérlő ellen; a délutáni szakasz kézi vezérlésűnek tűnt	Huntress – megerősített
2026. okt. 16.	A Huntress riaszt; 19:00-kor 162 igazolt bérlő	Huntress, iNews – megerősített
2026. okt. 16., 17:48	ConnectWise: „vizsgálat folyamatban”, korlátozó intézkedések érvényben	ConnectWise státuszoldal – megerősített
2026. okt. 17., 05:11	ConnectWise megerősíti az alkalmazásidentitásokhoz való jogosulatlan hozzáférést, lekapcsolja a Cloud Backup-hozzáférést	ConnectWise státuszoldal – megerősített
2026. okt. 17., 07:00	Hét alkalmazásidentitás letiltva	ConnectWise státuszoldal – megerősített
2026. okt. 17.	A Microsoft nyilvánosan „aktív ellátásilánc-támadásnak” nevezi; sajtóban 173 bérlő	BleepingComputer, The Hacker News – jelentett
2026. okt. 18.	SaaS Security és Cloud Management is offline; további indikátorok közzététele, kármentési útmutató a partnereknek	ConnectWise státuszoldal – megerősített
2026. okt. 18.	Néhány sikertelen felhasználói bejelentkezés egy újabb címről, ugyanabból a hosting-tartományból	Huntress, The Hacker News – megerősített
2026. okt. 19., 01:28	Szolgáltatások továbbra is felfüggesztve, visszaállítási idő nincs; a partnerek tartásák letiltva az alkalmazásokat	ConnectWise státuszoldal – megerősített
2026. okt. 19.	ConnectWise: fiókok visszaállítva, alkalmazás-hitelesítő adatok lecserélve, külső incidenskezelők bevonva; nincs sikeres támadói aktivitás okt. 17., 05:00 óta	The Hacker News , okt. 20. , ConnectWise státuszoldal – megerősített
2026. okt. 19., 17:30 (13:30 ET)	Huntress-frissítés: 10 000+ bérlő átnézve, második kompromittált bérlő, nincs postafiók- vagy fájlmodosítás; utolsó igazolt sikeres támadói belépés okt. 15., 08:44	Huntress – megerősített
2026. okt. 20.	A szolgáltatások még mindig állnak, visszaállítási idő nincs	ITPro , okt. 20. , The Hacker News , okt. 20. – megerősített

Dátum (UTC)	Esemény	Forrás
2026. okt. 20., 13:01 és 19:05	ConnectWise: kétóránkénti partner-webinárok; szakaszos visszaállítás előkészítése, „több nap”	ConnectWise státuszoldal – megerősített
2026. okt. 21.	A Microsoft a támadást a Storm-0940-nek tulajdonítja, ARTEX AI-keretrendszer használatával; 2250+ megcélzott bérlő	Microsoft; The Record; The Hacker News – megerősített (Microsoft-értékelés)
2026. okt. 21., 14:35	ConnectWise: megkezdődött a szolgáltatások szakaszos visszaállítása, biztonsági ellenőrzéshez kötve	ConnectWise státuszoldal; Infosecurity Magazine – megerősített
2026. okt. 22.	A visszaállítás folyamatban, napi két státuszfrissítés; szolgáltatásonkénti újrapcsolási utasítás még nincs	ConnectWise státuszoldal – megerősített

Szereplők és háttér

- **ConnectWise:** amerikai szoftvergyártó, amely kifejezetten managed service providereknek (MSP-knek, vagyis külsős rendszergazda-cégeknek) fejleszt távfelügyeleti, jegykezelő, mentési és biztonsági eszközöket. Egy MSP egyetlen ConnectWise-konzolról tucatnyi vagy száznyi ügyfelet kezel. A cég termékei korábban is támadások célpontjai voltak, például a ScreenConnect távelérési szoftver 2024. februári sebezhetősége (CVE-2024-1709) miatt. **[megerősített: ConnectWise Trust Center]**
- **SkyKick:** Microsoft 365-migrációs és -mentési szolgáltató, főleg MSP-knek; 2024 óta a ConnectWise része. A régebbi bérlőkben az alkalmazások még „SkyKick” néven szerepelhetnek. **[megerősített: BleepingComputer, Blumira]**
- **Huntress:** MSP-k számára biztonsági megfigyelést nyújtó cég; ő vette észre és publikálta a legrészletesebb elemzést. Egyben maga is érintett: a támadó a Huntress alkalmazásához is kulcsot adott egy bérlőben, amit a cég eltávolított. **[megerősített: Huntress]**
- **Microsoft:** a saját telemetriája alapján megerősítette a gyanús IP-ről érkező széles körű alkalmazás-hitelesítést, és ellátáslánc-támadásnak minősítette. **[jelentett: BleepingComputer, The Hacker News]**
- **Sophos X-Ops (új forrás, 2026-10-20):** saját telemetriájában ugyanazt a szkriptelt végigsöprést látta (október 15., 07:11–08:47 UTC, egyetlen VPS-ről), és megfigyelte, hogy a támadó olyan bérlőket is végigjárt, ahol nem volt aktív mentési előfizetés, vagyis valószínűleg az alkalmazást valaha jóváhagyó összes bérlő listáját használta. **[megerősített: Sophos X-Ops]**
- **Todyl, SpecterOps, Blumira, Coalition:** független biztonsági cégek és egy kiberbiztosító, amelyek saját ügyfélkörükön elemezték az esetet és ellenőrzési útmutatót adtak ki.
- **Elkövető – Storm-0940 (frissítve: 2026-10-23):** a Microsoft által 2021 óta követett, kínai állami érdekekhez igazodó csoport, amelyet a cég először 2024 novemberében írt le részletesen; jellemző módszere a jelszószórás, az internetre nyitott alkalmazások kihasználása, és a meglévő OAuth-alkalmazásokhoz adott új hitelesítő adatokkal való megkapaszkodás. Célpontjai a Microsoft szerint többek között a védelmi és repülőgépipar, az energia, a pénzügyi szolgáltatások, a kormányzat, a jogi szektor, a félvezetőipar és az agytrösztök. *(korábban: „ismeretlen”)* **[megerősített mint Microsoft-értékelés: Microsoft; Infosecurity Magazine; The Hacker News]**
- **ARTEX:** nyílt forrásként, 2026 elején GitHubon kiadott, Go nyelvű, többügynökös AI-behatolásteszt-keretrendszer, amely tetszőleges nyelvi modellel működik; az ügynökök a felderítéstől az adatkivitelig önállóan végigvihetnek egy tesztet. Eredetileg engedélyezett tesztelésre készült; a fejlesztő október 8-án közölte, hogy visszaéltek vele, és a projektet zárt forrásúvá tette. A Zscaler október 14-én egy dél-koreai pénzintézetek elleni, pénzügyi motivációjú kampányban írta le a

használatát; a Microsoft szerint több régióban több csoport is használja. **[megerősített: Microsoft, Zscaler ThreatLabz, The Record]**

- **Kína reakciója:** a The Record a Reutersre hivatkozva azt írja, hogy a kínai külügyminisztérium szóvivője tagadta, hogy tudna az incidensekről; a cikkből nem egyértelmű, hogy ez a ConnectWise-hozzárendelésre vagy a korábbi, ARTEX-szel kapcsolatos esetekre vonatkozott. **[jelentett: The Record]**

Előzmények: ez nem az első „egy kulcs, sok ajtó” eset

- **Kaseya VSA, 2021. július 2.:** a REvil zsarolóvírus-csoport a Kaseya helyben telepített távfelügyeleti szoftverének nulladik napi hibáin keresztül kb. 50–60 MSP-n át 800–1500 végső ügyfélcéget titkosított. A minta ugyanaz: az MSP eszköze egyetlen ponton át sok céghez ad hozzáférést. **[megerősített: TechTarget]**
- **Midnight Blizzard a Microsoftnál, 2024. január:** egy orosz állami csoport egy régi, MFA nélküli tesztbérletről egy elfelejtett, de magas jogosultságú OAuth-alkalmazást vett át, és azzal postafiókokhoz jutott. A tanulság ugyanaz: a gépi identitások és a régi alkalmazás-engedélyek gyakran kívül esnek a figyelmen. **[megerősített: Microsoft]**
- **Salesloft Drift, 2025. augusztus:** az UNC6395 néven követett csoport egy csevegőbot-integráció ellopott OAuth-tokenjeivel számos cég Salesforce-adatát töltötte le. A Google azt javasolta, hogy minden, a Drifthez kötött tokent tekintsenek kompromittáltnak. **[megerősített: Google GTIG a Security Affairs szerint]**
- **Trend:** a támadók egyre inkább nem a jelszót, hanem a szolgáltatások közötti „gépi bizalmat” (OAuth-alkalmazások, API-kulcsok, tokenek) célozzák, mert az MFA ott nem véd, és a naplózás is gyengébb. **[feltételezés, a fenti három eset és a SpecterOps elemzése alapján]**

Hogyan működik

RED // TÁMADÓI SZEMMEL

Fogalmi szinten, miért működhetett:

1. **A kulcs a gyártónál van, nem nálad.** Amikor egy MSP bekapcsolja a felhőmentést, a Microsoft 365 rendszergazdája egyszer jóváhagyja („consent”), hogy a mentőalkalmazás olvashassa a teljes levelezést és fájlállományt. Ettől kezdve az alkalmazás a gyártó saját kulcsával bármikor tokent kérhet. A Huntress szerint ezt a hitelesítő adatot semmi nem állíthatta elő, amit az ügyfél a saját környezetében tett. **[megerősített: Huntress]**
2. **Egy kulcs minden zárba.** A multi-tenant alkalmazásnak egy identitása van, amely minden olyan bérlőben működik, ahol jóváhagyták. Aki ezt megszerzi, egy listán végigmehet az összes ügyfélen; a naplók szerint a támadó pontosan így tett, automatizáltan, rendezett sorrendben. **[megerősített: Huntress, Todyl]**
3. **Nincs ember, nincs MFA.** Gép jelentkezik be géphez, így a felhasználókra szabott védelmek (MFA, kockázatos bejelentkezés, eszközmegfelelőség) nem lépnek életbe. A feltételes hozzáférés (Conditional Access) külső, multi-tenant alkalmazásra korlátozottan alkalmazható. **[megerősített: SpecterOps, Todyl, Blumira]**
4. **A rosszindulatú forgalom úgy néz ki, mint a normál mentés.** Egy mentőszoftvernek az a dolga, hogy tömegesen olvasson leveleket és fájlokat. A támadó ugyanazzal az identitással ugyanezt teheti, ezért az aktív mentést használó bérlőkben a Todyl szerint nem lehetett szétválasztani a legitim és a támadói olvasást. **[megerősített: Todyl, Coalition]**

5. **A naplók hiányosak.** A Graph-on keresztüli könyvtárolvasás nem mindig hagy auditnyomot, az alkalmazásszintű műveleteknél az audit napló nem rögzíti a forrás-IP-t, az ingyenes Entra ID csak 7 napig őriz naplót, a részletes Graph-tevékenységnapló pedig külön bekapcsolandó (P1/P2 licenc) és nem visszamenőleges. **[megerősített: Huntress, Todyl, Blumira]**
6. **Kitartás más alkalmazásokon keresztül.** Ha egy megbízható alkalmazás rendszergazdai szerepet kap, más alkalmazásokhoz is adhat új titkos kulcsot. Így a támadó akkor is visszajöhet, ha az eredeti kulcsot visszavonják: ezért nem elég csak a ConnectWise-alkalmazást letiltani. **[megerősített: Huntress, SpecterOps]**
7. **A letiltás nem azonnali.** A már kiadott tokenek a letiltás után még legfeljebb kb. 60–90 percig érvényesek. A felhasználói munkamenetek visszavonása erre nem hat. **[megerősített: Todyl, Blumira]**
8. **Gépi sebesség (új, 2026-10-23).** A Microsoft szerint a támadó AI-ügynököket használt, amelyek nem fáradnak, éjjel-nappal dolgoznak, és egyszerre több behatolási utat próbálnak végig. Ez nem új technikát jelent, hanem a meglévők (felderítés, jelszószórás, alkalmazásjogokkal való visszaélés) felgyorsítását: a Microsoft szerint több esetben három óránál kevesebb idő telt el a célba vételtől a kiemelt jogosultságig, ami az emberi védekezőknek alig hagy reakcióidőt. A tanulság: ahol a védekezés kézi riasztás-feldolgozásra épül, ott a megelőzés (szűk jogosultság, rövid életű kulcsok) többet ér, mint a gyors észlelés. **[megerősített: Microsoft; The Record; értelmezés: feltételezés]**

A gyengeség tehát nem egy klasszikus „lyuk”, hanem a bizalmi lánc tervezése: széles, állandó jogosultság, egyetlen közös kulcs, gyenge láthatóság. Ezt a Promptly Secured-szög így foglalhatja össze: *a te kulcsod a szolgáltató kulcskarikáján lóg.*

Hatás és magyar vonatkozás

Ismert hatás:

- 162 → 173 igazolt bérlő jogosulatlan bejelentkezéssel; közel 1000 bérlőben kísérlet, 300-nál több sikeres bejelentkezés (Huntress, a ConnectWise-on kívüli látókörével). Egy szervezet több bérlőt is működtethet, ezért a bérlőszám nem egyenlő a cégek számával. **[jelentett: Huntress, tech-insider]**
- A Microsoft szerint a Storm-0940 a ConnectWise-hozzáféréssel több mint 2250 bérlőt célzott meg; a kísérletek többsége sikertelen volt, de „sok szervezetnél” tartós, kiemelt hozzáférést ért el, ahol pedig továbbjutott, ott felderítést, alkalmazás-hitelesítő adatok hozzáadását és szerepkör-, csoport- és identitásmódosításokat végzett. A Microsoft hangsúlyozza: egy érintett alkalmazás vagy sikeres bejelentkezés jelenléte önmagában nem jelenti, hogy ügyfeladathoz hozzáfértek vagy azt kivítették. (új, 2026-10-23) **[megerősített: Microsoft; Infosecurity Magazine]**
- Ügyvédi irodák (jelszószórás) és stratégiai ágazatok (második hullám) a kiemelt célpontok között; a Microsoft által felsorolt célágazatok (védelmi ipar, kormányzat, energia, pénzügy, jog, félvezetőipar, agytrösztök) ezzel egybevágnak. **[megerősített: Huntress, Microsoft]**
- Az adatkiszivárgás mértéke ismeretlen. A Huntress a két általa vizsgált kompromittált bérlőben nem talált postafiók- vagy fájlmodosítást, de a Graph-olvasás nem hagy nyomot (frissítve: 2026-10-20); korábban egyes MSP-k a Redditen e-mail-, Teams- és SharePoint-adatok kimásolásáról számoltak be, ezt sem a ConnectWise, sem a Huntress nem erősítette meg. A Todyl kilenc, mentési előfizetés nélküli bérlőben csak bejelentkezést és felderítést látott, további aktivitást nem. **[jelentett: Blumira, Coalition; megerősített: Todyl]**
- **Mellékhatás: mentés nélkül maradt cégek.** Az óvintézkedések miatt a Cloud Backup-ügyfelek október 17. óta nem mentettek és nem tudtak visszaállítani; október 21-én megkezdődött a

szakaszos visszaállítás, de október 22-én a teljes helyreállítás még „több napig” tart *(korábban: október 20-án visszaállítási időpont nélkül; frissítve: 2026-10-23)*. A Coalition kiberbiztosító figyelmeztet: ha ebben az ablakban egy másik incidens (például zsarolóvírus) történik, a helyreállítás nehezebb. **[mege erősített: ConnectWise státuszoldal; Coalition]**

- **Koncentrációs kockázat:** a Coalition szerint egy MSP jellemzően egy mentési gyártót használ minden ügyfelénél, így egy gyártói incidens egyszerre sok biztosított kárt okozhat. **[feltételezés: Coalition]**

Magyar és régiós vonatkozás:

- **Magyar érintettség nem ismert.** A 2026. október 19-i, 20-i és 23-i kereséskor sem magyar hatósági (NBSZ NKI, SZTFH) figyelmeztetést, sem magyar sajtócikk nem volt elérhető az esetről, a Storm-0940-hozzárendelésről sem. A Microsoft elemzése „globális” célzásról ír, országot vagy régiót nem nevez meg; Európa és Magyarország nem szerepel benne. *(frissítve: 2026-10-23)* Országos bontást egyik forrás sem közölt; az iNews kifejezetten jelzi, hogy ausztrál és európai számot sem ismer. **[mege erősített hiány a vizsgált forrásokban]**
- Mivel a SkyKick/ConnectWise kifejezetten MSP-csatornán értékesít, és a Microsoft 365 a magyar kkv-knál is elterjedt, nem zárható ki, hogy magyar MSP-k ügyfelei is érintettek. **[feltételezés]**
- **Szabályozási szög:** a NIS2 hazai átültetése szerint az érintett cégek felelősek ellátási láncuk informatikai biztonságáért, és a Portfolio idézte szakértő szerint a kiszervezés nem viszi át a felelősséget: „a végső felelősség a szolgáltatást igénybe vevő szervezetet terheli”. A legtöbb cég felügyeleti hatósága az SZTFH. **[jelentett: Portfolio]**

Mit tegyél

BLUE // MIT TEGYÉL MOST

Magánszemély (aki céges vagy kisvállalkozói Microsoft 365-öt használ)

- Kérdezd meg a cég IT-sát vagy rendszergazdáját: használunk-e ConnectWise Cloud Backupot vagy SkyKicket, és megtörtént-e a letiltás és az ellenőrzés?
- Ha saját vállalkozásod van egy MSP-vel: kérj tőlük írásos visszajelzést az alábbi kisvállalkozói pontokról.
- Légy óvatos a következő hetekben az ismerős hangú, de szokatlan kérést tartalmazó e-mailekkel (például számlaszám-változás, sürgős utalás). Ha valaki a levelezéshez hozzáfért, abból hiteles csalóleveleket írhat. Kétes esetben hívd fel a feladót egy ismert számon. **[feltételezés, általános óvatossági elv]**

Kisvállalkozás (Microsoft 365-bérlő, külsős IT-partnerrel)

- Kérd meg az MSP-t, hogy keressen rá a bérlődben az összes ConnectWise- és SkyKick-alkalmazásra, *akkor is, ha már régen nem használják*, és tiltsa le őket (letiltás, ne törlés), amíg a ConnectWise nem igazolja a kulcsok cseréjét. **[Huntress, Todyl, Blumira]**
- A letiltás előtt mentsék ki az alkalmazás engedélylistáját és a naplókat: az ingyenes Entra ID csak 7 napig őriz naplót. **[Todyl, Blumira, Coalition]**
- Kérdezd meg: kaptak-e ezek az alkalmazások rendszergazdai szerepet, és került-e bármely alkalmazásra új titkos kulcs vagy tanúsítvány 2026. október 13. óta? **[Huntress]**
- Gondoskodj ideiglenes mentésről (október 21-én elindult a szakaszos visszaállítás, de a teljes helyreállítás „több napig” tart; frissítve: 2026-10-23): amíg a Cloud Backup áll, legyen legalább egy

másik, friss mentés a kritikus postafiókokról és fájlokról. **[Coalition, ConnectWise státuszoldal alapján]**

- Ha kiberbiztosításod van, nézd meg, kell-e bejelentened a gyanús aktivitást, és őrizd meg a naplót. **[Coalition]**
- Hosszabb távon kérdezd meg az MSP-t: milyen külső alkalmazásoknak adott a nevemben bérlőszintű jogot, és melyikre van valóban szükség? Ezt kérd évente, írásban.

Szervezet (saját IT-val, vagy MSP-ként)

- **Azonnal:** a Cloud Backup-alkalmazás és a Teams Cloud Management-alkalmazás letiltása minden bérlőben; a többi ConnectWise/SkyKick Cloud Management-alkalmazásé is, amíg a gyártó nem ad formális visszaállítási utasítást. **[Huntress, ConnectWise]**
- **Naplóvizsgálat:** az Entra „Service principal sign-ins” fülén (nem a felhasználói bejelentkezéseknél!) szűrj az alkalmazásazonosítóra, és keresd a nem Microsoft/Azure tartományból érkező hitelesítést; október 1-ig vagy ameddig a megőrzés engedi. **[Huntress, Todyl, ConnectWise]**
- **Auditnapló:** szerepkör-hozzárendelések, hozzájárulások (consent) és új hitelesítő adatok minden alkalmazáson október 13. óta, különös figyelemmel a felügyeleti és biztonsági eszközökre. A nem szándékosan adott globális rendszergazda- és Privileged Authentication Administrator-szerepeket vond vissza. **[Huntress]**
- **Unified audit log:** levél-, fájl- és Teams-olvasási események, ahol a kliensalkalmazás az érintett alkalmazás; szokatlan tömeges olvasás a mentési ütemezésen kívül; új postafiókszabályok és -engedélyek. **[Todyl, Coalition, Blumira]**
- **Ne kapsd vissza idő előtt (új, 2026-10-20):** az érintett alkalmazásokat csak a ConnectWise formális visszaállítási utasítása után engedélyezd újra; a gyártó szerint a letiltás csak az új kapcsolódást akadályozza meg, a bérlőben korábban végzett változtatásokat nem fordítja vissza. Az ellenőrzést október 13-tól, de lehetőleg október 1-től végezd, a régóta nem használt („alvó”) SkyKick-kapcsolatokra is. **[ConnectWise a ITPro, okt. 20. és a The Hacker News, okt. 20. szerint; Infosecurity Magazine]**
- **A Microsoft vizsgálati ajánlása (új, 2026-10-23):**
 - Ne töröld első lépésben az érintett vállalati alkalmazásokat: előbb mentsd a konfigurációt és a bizonyítékokat (Entra bejelentkezési és auditnaplók, Purview-audit, SIEM, Graph-telemetry), de a mentésre várva ne halaszd a letiltást.
 - Az alkalmazásokat azonosító (application ID) alapján keresd, ne megjelenítési név szerint, és jegyezd fel bérlőnként a helyi service principal objektumazonosítóját.
 - Nézd át minden bérlőt, ahol az alkalmazást valaha telepítették vagy jóváhagyták, akkor is, ha nem használják.
 - A sikeres és a sikertelen service principal-bejelentkezéseket külön vizsgáld, legalább október 15-től, a service principal-bejelentkezéseknél október 1-ig visszamenőleg; ne csak a közzétett IP-címekre szűrj, hanem minden, a gyártó megszokott infrastruktúráján kívüli forrásra.
 - Az auditnaplóban keresd: új hitelesítő adatok, új alkalmazások, service principalok vagy tulajdonosok, alkalmazásszerepkör-hozzárendelések, hozzájárulások, kiemelt szerepkör-változások, felhasználó-, csoport-, hitelesítésmódszer- és feltételes hozzáférési módosítások.
 - Ha Azure Key Vaultot használsz, nézd meg a szokatlan tömeges titkolvasást is.
 - A bizonyítékok mentése után egy jogosult incidenskezelő távolítsa el az igazoltan jogosulatlan hitelesítő adatokat, jóváhagyásokat, tulajdonosokat és hozzárendeléseket, és cserélje a kulcsokat ott, ahol gyanús aktivitás volt.
 - Ellenőrizd, hogy a gyártói kulcscsere és a bérlőszintű kármentés valóban megszüntetett-e minden jogosulatlan hozzáférést. **[megerősített: Microsoft]**

- **Újrakapcsoláskor (új, 2026-10-23):** csak a ConnectWise szolgáltatásonkénti, formális utasítása alapján kapcsold vissza az alkalmazásokat; október 22-én ilyen utasítás még nem jelent meg. Az újrakapcsolás előtt legyen kész a fenti átvizsgálás. **[ConnectWise státuszoldal, Microsoft]**
- **Láthatóság:** kapcsold be a Microsoft Graph-tevékenységnaplót (nem visszamenőleges), és növeld a naplómegőrzést. **[Huntress, Todyl]**
- **Keményítés:** alkalmazáskezelési szabályzatokkal korlátozd a titkos kulcsok használatát és élettartamát; szűkítsd az Application Administrator és Cloud Application Administrator szerepek körét; ahol a licenc engedi, használj feltételes hozzáférést és Entra ID Protection munkaterhelés-identitásokra; Exchange-ben alkalmazás-RBAC-kal korlátozd, mely postafiókokhoz férhet egy alkalmazás. **[Huntress, Microsoft]**
- **Harmadik fél kockázat (TPRM):** vezess nyilvántartást minden multi-tenant alkalmazásról, annak engedélyeiről és gazdájáról; az MSP-szerződésben rögzítsd az incidensértesítést, a hozzáférések korlátozását, a naplózást és a szerződés végén a hozzáférések visszavonását. **[ASD/CISA/NCSC közös ajánlás: cyber.gov.au; Portfolio]**
- **Kiszervezés-exit:** a számla lemondása nem szünteti meg a gyártó hozzáférését; az alkalmazásengedélyt külön vissza kell vonni. **[Blumira]**

Szakmai blokk

- **CVE:** nincs. Jelenlegi ismeretek szerint hitelesítőadat-kompromittálás, nem publikált sebezhetőség; a ConnectWise szerint még nem tudni, közrejátszott-e termékhiba. **[The Hacker News]**
- **Érintett komponensek:** ConnectWise Cloud Backup (SkyKick) Microsoft 365 enterprise alkalmazás, valamint a Cloud Management alkalmazáscsalád (MS Teams, Exchange Online, MS Graph, Partner Center, SharePoint Online). A ConnectWise összesen hét alkalmazásidentitást tiltott le. Régebbi bérlőkben „SkyKick Cloud Manager” név alatt is szerepelhetnek. **[ConnectWise, BleepingComputer]**
- **Hitelesítési folyamat:** OAuth 2.0 client credentials (alkalmazásszintű, app-only token), clientAssertion típusú hitelesítéssel, a gyártói bérlőben tárolt kulccsal. **[Huntress, Todyl]**
- **Kihasznált engedélyek:** a Microsoft szerint valószínűleg a Directory.ReadWrite.All; a Todyl szerint levél-, fájl-, Teams-írás/olvasás és EWS teljes postafiók-hozzáférés. **[BleepingComputer, Todyl]**
- **MITRE ATT&CK (Huntress szerint):**
 - T1078.004 – Valid Accounts: Cloud Accounts (a gyártói kulcs használata)
 - T1098.003 – Account Manipulation: Additional Cloud Roles (önkiosztott globális és Exchange-rendszergazda)
 - T1098.001 – Account Manipulation: Additional Cloud Credentials (titkos kulcs más alkalmazásokra)
 - Kiegészítésként: T1110.003 Password Spraying (október 13–14.) **[a leírt viselkedés alapján: feltételezés]**
 - **A Microsoft október 21-i elemzése szerint továbbá (frissítve: 2026-10-23):** T1595 Active Scanning; T1195 Supply Chain Compromise; T1199 Trusted Relationship *(korábban: feltételezés; most a Microsoft is felsorolja)*; T1528 Steal Application Access Token; T1555.006 Cloud Secrets Management Stores (tömeges Key Vault-titkolvasás); T1087.004 Cloud Account; T1580 Cloud Infrastructure Discovery. **[megerősített: Microsoft]**
- **Microsoft Defender-észlelések (fogalmi):** alkalmazás önmagának adott globális rendszergazdai szerepet; bejelentkezés ismert támadói, illetve igazolt állami infrastruktúrából; gyanús alkalmazásszerepkör-hozzárendelés service principalhoz; Key Vault-hozzáférési anomália. A

Microsoft vadászati (advanced hunting) és Sentinel-lekérdezéseket is közzétett. **[megerősített: Microsoft]**

- **Észlelési ötletek (fogalmi):**

- Service principal-bejelentkezések, ahol a forrás nem a gyártó megszokott (Azure privát IPv6) kimenete, hanem nyilvános hosting-szolgáltató.
- Alkalmazás, amely saját magát szerepkörhöz rendeli, vagy másik alkalmazáshoz hitelesítő adatot ad.
- A felhasználói ügynök (User-Agent) és a művelet kombinációja: a ConnectWise saját alkalmazásai más ügynökökkel futnak, mint a támadói szkriptek; önmagában egyik ügynök sem megbízható jelzés. **[Huntress]**
- Gráfalapú elemzés (pl. BloodHound/AzureHound) a külső alkalmazásoktól a legmagasabb jogosultságú (Tier Zero) erőforrásokig vezető utak feltérképezésére. **[SpecterOps]**

- **Indikátorok típusa és hivatalos forrása:** IP-címek (egy hosting-szolgáltató tartományából, a ConnectWise október 18-án továbbiakat tett közzé; a Microsoft október 21-én átmeneti VPN-címeket is közölt), alkalmazásazonosítók, gyártói bérlőazonosító, felhasználói ügynökök, munkamenet-azonosító minta. Teljes lista: [Microsoft](#), [Huntress](#), [Todyl](#), [ConnectWise státuszoldal](#). Fontos: a Cloud Backup-alkalmazás azonosítója *legitim*, nem szabad tiltólistára tenni, csak letiltani az alkalmazást. **[Huntress]**
- **Hivatalos ajánlások:** ConnectWise kármentési útmutató a partnereknek (státuszoldalon hivatkozva), Huntress-, Todyl- és SpecterOps-útmutatók; háttérként a Microsoft Midnight Blizzard-útmutatója az OAuth-alkalmazások visszaélései ellen, és az ASD/CISA/NCSC/NSA/FBI közös MSP-tanácsadása.

Ellentmondások és nyitott kérdések

Nyitott kérdések

- **162 vagy 173?** A Huntress blogja 162-t ír (október 16., 19:00 UTC); a The Hacker News és több másodlagos oldal 173-at (október 17.), a Huntressnek tulajdonítva, de a Huntress-blogban a 173 október 23-án sem szerepel. A Microsoft október 21-én egy harmadik, más jellegű számot közölt: 2250+ *megcélzott* bérlő. Összefoglalva: „legalább 162 bérlőben igazolt a belépés; a Microsoft szerint 2250-nél több bérlőt próbáltak elérni”. *(frissítve: 2026-10-23)*
- **Mikor tudott róla a ConnectWise?** A források szerint október 14-én (The Hacker News), október 15-én (Infosecurity Magazine, SecurityWeek), illetve október 16-án (ITPro); a státuszoldal első bejegyzése október 16., 17:48 UTC. Továbbra sem dönthető el. Biztosan annyi mondható: „a gyártó október 16-án tájékoztatott nyilvánosan”.
- ~~Letiltották-e mindet?~~ **Lezárva (2026-10-20):** időbeli eltérés volt; a Huntress október 17-i frissítése szerint a ConnectWise addigra megerősítette a letiltást.
- **Az időablak:** Huntress 06:13–08:34, Todyl és Sophos 07:11–08:47 UTC (eltérő ügyfélkörök) – nem ellentmondás; összefoglalva: „október 15. kora reggel (UTC)”.
- **„A mentett adat nem sérült” – de az élő adat?** A ConnectWise az *archívumokról* nyilatkozott, és október 21–22-én is hangsúlyozza, hogy ez nem mond semmit az egyes ügyfélbérlők állapotáról. A Microsoft is úgy fogalmaz, hogy a sikeres bejelentkezés nem jelenti automatikusan az adat elérését vagy kivitelét.
- ~~Ki és miért?~~ **Részben lezárva (2026-10-23):** a Microsoft a Storm-0940-nek tulajdonítja, amely a cég szerint jellemzően adatlopásra törekszik. Ez egyetlen cég értékelése, formális bizonyossági szint nélkül; a ConnectWise státuszoldala nem kommentálja, és a sajtó is eltérően írja le a gyártó reakcióját (The Next Web: nem reagált; Infosecurity Magazine: frissítést adott ki, amely elismeri a

Microsoft megállapításait). Ezért a Promptly Secured így fogalmaz: „a Microsoft szerint egy kínai állami érdekekhez igazodó csoport”.

- **A „három óra” mire vonatkozik?** A Microsoft a tágabb, szeptember óta tartó ARTEX-kampányra írja, hogy több esetben három óránál rövidebb idő telt el a célba vételtől a kiemelt jogosultságig; a szövegből nem egyértelmű, hogy ez konkrétan ConnectWise-ügyfélbérlelőkre is igaz-e. Ezért a kampányra vonatkoztatva közöljük. (új, 2026-10-23)
- **Mennyit számított az AI?** A felderítés, a jelszószórás és az alkalmazásjogokkal való visszaélés ismert technikák; az AI-ügynökök a Microsoft szerint a sebességet és a párhuzamosságot adták hozzá. Hogy melyik modellt használták, a Microsoft nem közölte, és független szakértői értékelést az AI-szerepről a vizsgált források nem tartalmaznak. (új, 2026-10-23)
- **Hogyan került ki a kulcs?** Továbbra sem ismert; a ConnectWise független szakértőkkel vizsgálja, a Microsoft sem írja le.
- **Kiszivárgott-e adat?** Továbbra sem ismert; a Huntress két vizsgált bérlelőjében nincs módosítás, a Microsoft ahol továbbjutottak, felderítést és jogosultság-módosítást látott, adatkivitel ebben a kampányban nem erősített meg.
- **Mikor jön vissza teljesen a mentés, és mi lesz az újrapcsolási utasítás?** A szakaszos visszaállítás október 21-én elindult; szolgáltatásonkénti utasítás október 22-én még nem volt.

Forrásértékelés

Forrás	Típus	Megbízhatóság	Mit támaszt alá
Huntress blog	kutató (elsődleges)	magas	idővonal, 162 bérlelő, technikák, ATT&CK, második hullám, ajánlások, IOC-k
ConnectWise státuszoldal	cég (elsődleges)	magas (a saját állításairól)	gyártói lépések, szolgáltatásállapot, archívumok állapota
Todyl	kutató (elsődleges)	magas	engedélyek, token-élettartam, 9 bérlelő elemzése, észlelés
SpecterOps	kutató	magas	MFA-megkerülés magyarázata, támadási utak, ellenőrzés
BleepingComputer	sajtó	magas	Microsoft-értékelés, idővonal, ConnectWise-nyilatkozatok
The Hacker News – 173 bérlelő	sajtó	közepes–magas	173-as szám, összefoglaló
The Hacker News – felfüggesztés	sajtó	közepes–magas	~1000/300 bérlelő, okt. 14-i azonosítás, letiltási ellentmondás
iNews	sajtó	magas	ConnectWise-nyilatkozat okt. 19., regionális adat hiánya
Coalition	cég (biztosító)	közepes–magas	biztosítási és koncentrációs kockázat, helyreállítási hatás
Blumira	cég (biztonsági gyártó)	közepes	kkv-specifikus kockázatok, naplómegőrzés, MSP-beszámolók
tech-insider	sajtó (másodlagos)	alacsony–közepes	a 173-as szám eredete (ellentmondásos)
Microsoft – Midnight Blizzard	cég (elsődleges)	magas	előzmény, OAuth-védekezés
Security Affairs – Salesloft Drift	sajtó	közepes–magas	előzmény (2025)
TechTarget – Kaseya	sajtó	magas	előzmény (2021)
cyber.gov.au – MSP-tanácsadás	hatóság	magas	MSP-ügyfelek teendői

Forrás	Típus	Megbízhatóság	Mit támaszt alá
The Hacker News– hitelesítő adatok cseréje (okt. 20.)	sajtó	közepes–magas	okt. 19-i gyártói kármentés, Huntress 10 000+ bérlő, új IP-k
ITPro (okt. 20.)	sajtó	magas	harmadik nap állapota, „letiltás nem fordít vissza”, okt. 1-ig visszamenő ellenőrzés
Sophos X-Ops	kutató (elsődleges)	magas	független megerősítés, előfizetés nélküli bérlők is a listán
SecurityWeek	sajtó	magas	szolgáltatás-leállítások sorrendje, CoreView-idézet
Infosecurity Magazine	sajtó	magas	ConnectWise-ajánlások, attribúció hiánya
Portfolio – NIS2	sajtó (magyar)	közepes	NIS2 ellátási lánc, SZTFH
Microsoft Security Blog – Storm-0940/ARTEX (okt. 21.)	cég (elsődleges)	magas (a saját értékeléséről)	hozzárendelés, ARTEX-használat, 2250+ bérlő, idővonal, vizsgálati ajánlás, ATT&CK, IOC-k
The Record (okt. 22.)	sajtó	magas	hozzárendelés átvétele, ARTEX-fejlesztő nyilatkozata, kínai tagadás
The Hacker News – ARTEX (okt. 22.)	sajtó	közepes–magas	Storm-0940 háttere, jelszószórás-számok, szakaszos visszaállítás
Infosecurity Magazine – Microsoft-hozzárendelés	sajtó	magas	célágazatok, ConnectWise-nyilatkozatok, visszaállítás
Zscaler ThreatLabz (okt. 14.)	kutató (elsődleges)	magas	ARTEX leírása; a dél-koreai kampány (nem a ConnectWise-ügy)
The Next Web (okt. 22.)	sajtó	közepes	összefoglaló, a ConnectWise reakciójának hiánya, Microsoft: nem saját sebezhetőség

Változásnapló

- **2026. október 20. (v2):** A szolgáltatások október 17. óta állnak, a ConnectWise lecserélte a hitelesítő adatokat; a Huntress 10 000+ bérlő átnézése után egy második kompromittált bérlőt talált, de postafiók- vagy fájlmodosítást nem. Bővült az idővonal, a teendők (ne kapsd vissza idő előtt, ideiglenes mentés) és egy követő cikkszög.
- **2026. október 23. (v3):** A Microsoft október 21-én a támadást a kínai állami érdekekhez igazodó Storm-0940-nek tulajdonította, amely az ARTEX AI-ügynökös keretrendszert használta (2250+ megcélzott bérlő); bekerült a Microsoft vizsgálati ajánlása, a bővített ATT&CK-lista, és az, hogy a ConnectWise október 21-én szakaszosan elkezdte a visszaállítást. Új követő szög: gépi sebességű betörés.