مايكروسوفت تنسب اختراق ConnectWise Cloud Backup إلى المجموعة Storm-0940 المرتبطة بالصين



أعلنت مايكروسوفت أن Storm-0940، وهي مجموعة متوافقة مع الدولة الصينية، نفذت اختراق سلسلة التوريد لتطبيق ConnectWise Cloud Backup مستخدمةً إطار ARTEX للذكاء الاصطناعي الوكيلي.

- كشفت مايكروسوفت هذه النسبة يوم الأربعاء وحددت Storm-0940 كجهة التهديد.
- كان الهدف تطبيق ConnectWise Cloud Backup عبر اختراق سلسلة التوريد.
- استخدمت المجموعة ARTEX، وهو إطار اختبار اختراق وكيلي بالذكاء الاصطناعي مكتوب بلغة Go، لتسريع المسح وما يتصل به من أنشطة.
- أُغلق مصدر ARTEX لاحقًا بعد إساءة استخدامه ضد مؤسسات مالية في كوريا الجنوبية.
- لا يتضمن المقتطف مؤشرات فنية ولا أرقام CVE ولا عدد الضحايا.

ما الذي أُعلن

أفادت مايكروسوفت بأن Storm-0940، وهي جهة تصفها بأنها متوافقة مع الدولة الصينية، كانت وراء اختراق سلسلة التوريد الذي طال تطبيق ConnectWise Cloud Backup مؤخرًا. ووفق التقرير، استخدمت المجموعة إطار **ARTEX**، وهو إطار اختبار اختراق وكيلي بالذكاء الاصطناعي مكتوب بلغة Go، لتسريع عمليات المسح وما يرتبط بها أثناء الحادثة.

وذُكر أن الإطار أُغلق مصدره بعد إساءة استخدامه ضد مؤسسات مالية في كوريا الجنوبية. والمقتطف المتاح موجز ولا يتضمن مؤشرات اختراق ولا الإصدارات المتأثرة ولا أرقام CVE ولا عدد الضحايا.

أهمية الخبر

تجمع الحادثة بين أمرين يهمان الجهات المنظمة: الاعتماد على أدوات النسخ الاحتياطي والإدارة من أطراف خارجية، واستخدام المهاجمين وكلاء الذكاء الاصطناعي لتسريع الاستطلاع. وبما أن مؤسسات مالية كانت هدفًا لإساءة استخدام ARTEX سابقًا، فإن الخبر ذو صلة بالقطاع المالي في المملكة.

الخطوات المقترحة

على الجهات التي تستخدم ConnectWise Cloud Backup التعامل مع الخبر بوصفه دافعًا لمراجعة منظمة وهادئة لا حالة طوارئ. تابعوا التفاصيل الفنية الأوفى من مايكروسوفت وConnectWise، وتحققوا من تعرضكم عبر قنوات إدارة الموردين، وتجنبوا الافتراضات بشأن النطاق والأثر إلى حين صدور مزيد من المعلومات.

ما يجب فعله الآن

1. تحققوا مما إذا كان ConnectWise Cloud Backup مستخدمًا في بيئتكم، بما في ذلك لدى مزودي الخدمات المُدارة العاملين لصالحكم.
2. تواصلوا مع ConnectWise ومزودي الخدمة للتأكد من التعرض ولمعرفة أي إرشادات صدرت.
3. راجعوا الصلاحيات وبيانات الاعتماد الممنوحة لأدوات النسخ الاحتياطي وغيّروها إذا أوصى المورد بذلك.
4. تابعوا منشورات مايكروسوفت وConnectWise للحصول على مؤشرات الاختراق وأضيفوها إلى أدوات الكشف فور توفرها.
5. وثّقوا المراجعة في سجل مخاطر الأطراف الخارجية وأطلعوا رئيس أمن المعلومات واللجنة المعنية.