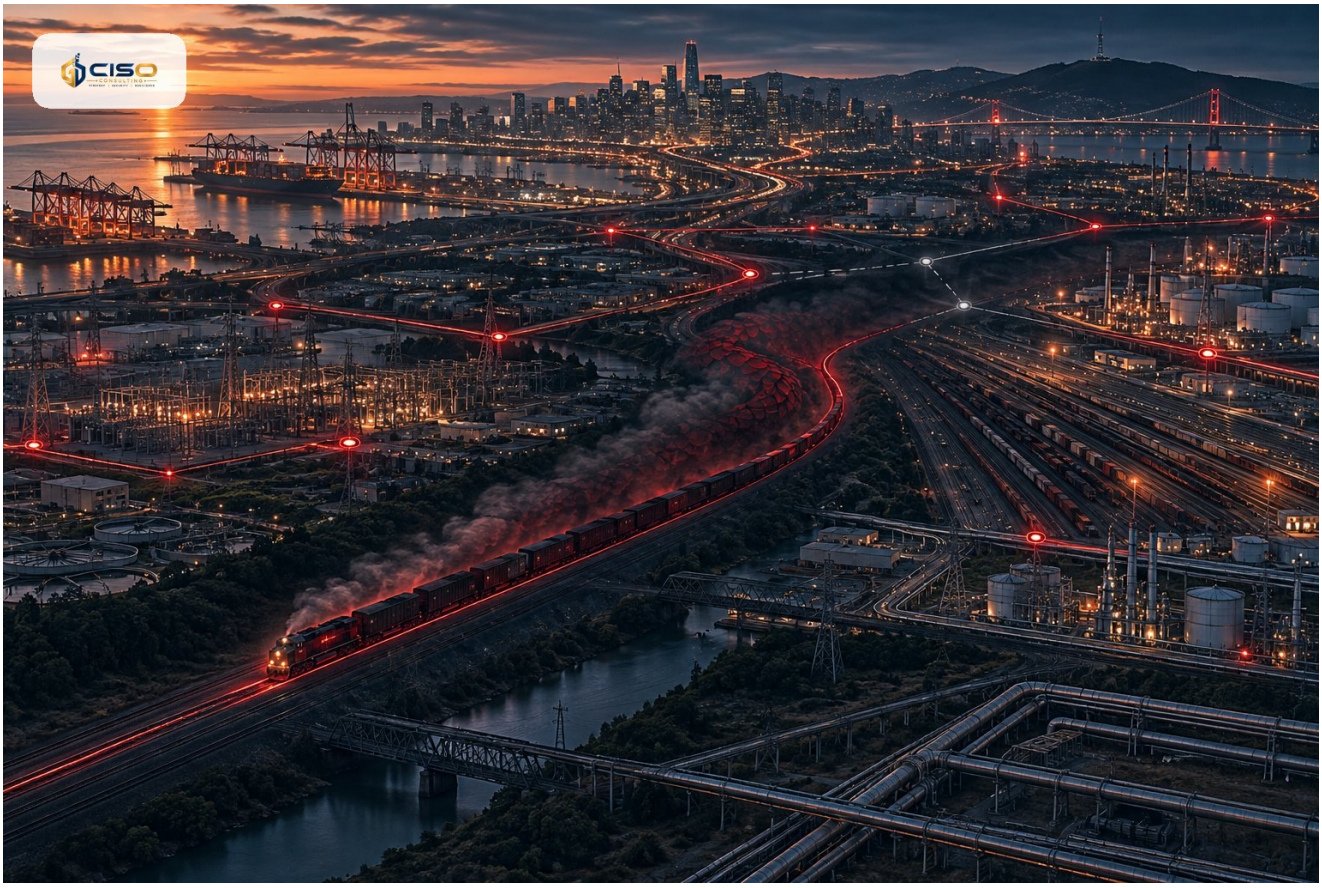
# ربط مجموعة Volt Typhoon بشبكة الوصول الخفية «Silent Train» التي جرى تعطيلها



نسب مختبر Black Lotus Labs التابع لـ Lumen شبكة وصول خفية تم تعطيلها تُدعى Silent Train إلى مجموعة Volt Typhoon المرتبطة بالصين، واستُخدمت لاستغلال الثغرات الصفرية والوصول الاستراتيجي.

- توصف Volt Typhoon بأنها مجموعة تجسس سيبراني مرتبطة بالصين.
- الشبكة الخفية المسماة Silent Train جرى تعطيلها.
- تفيد Black Lotus Labs التابعة لـ Lumen بأنها رُصدت أول مرة في أواخر 2023.
- تعتمد على سلاسل متبدلة من أجهزة SOHO وإنترنت الأشياء والبنية المؤسسية المخترقة.
- استُخدمت الشبكة لاستغلال الثغرات الصفرية وتحقيق وصول استراتيجي.

نسب مختبر Black Lotus Labs التابع لشركة Lumen Technologies شبكة وصول خفية تُدعى Silent Train إلى Volt Typhoon، وهي مجموعة تجسس سيبراني مرتبطة بالصين. وقد جرى تعطيل الشبكة. ووفق التقرير، استُخدمت في استغلال الثغرات الصفرية وفي تحقيق وصول استراتيجي.

## ما يصفه التقرير

يذكر المختبر أن Silent Train رُصدت أول مرة في أواخر 2023، وأنها تعمل عبر سلاسل متبدلة من أجهزة المكاتب الصغيرة والمنزلية (SOHO) وأجهزة إنترنت الأشياء والبنية التحتية المؤسسية المخترقة. وتمرير النشاط عبر سلاسل كهذه يصعّب تحديد مصدر الحركة الخبيثة.

ولا يتضمن المقتطف المتاح لنا تفاصيل أخرى، مثل المنتجات المتأثرة أو الضحايا أو مؤشرات الاختراق، لذلك لا نستنتج شيئاً في هذه النقاط.

## أهمية الخبر للجهات المنظمة

يذكّر استخدام أجهزة الحافة وإنترنت الأشياء المعتادة كنقاط تمرير بأن المعدات غير المُدارة أو سيئة الصيانة قد تصبح جزءاً من بنية هجومية يستخدمها طرف آخر. وتعطيل شبكة واحدة لا يزيل هذا الخطر الأوسع.

نوصي باعتبار الخبر دافعاً لمراجعة التعرض الذاتي، لا مؤشراً على تهديد محدد للجهة. ويُستحسن الاطلاع على تقرير Black Lotus Labs الكامل لمعرفة المؤشرات وإجراءات التخفيف.

## ما يجب فعله الآن

1. حصر أجهزة SOHO وإنترنت الأشياء والحافة المكشوفة على الإنترنت، بما فيها أجهزة الفروع والمواقع البعيدة.
2. تحديث أجهزة الحافة أو استبدال المنتهي دعمها منها، وإزالة أي تعرض خارجي غير لازم.
3. مراجعة السجلات بحثاً عن اتصالات واردة أو صادرة غير معتادة من أجهزة الحافة وإنترنت الأشياء.
4. الاطلاع على تقرير Black Lotus Labs الكامل وتطبيق المؤشرات المنشورة في المراقبة.
5. التأكد من جاهزية إجراءات الاستجابة للثغرات الصفرية، ومنها التخفيف الطارئ ومسارات التصعيد.