الاشتباه في استخدام مجموعة Webworm نسخة معدّلة من SoftEther VPN Bridge للوصول الخفي



يُشتبه في أن مجموعة Webworm المرتبطة بالصين تستخدم نسخة معدّلة من SoftEther VPN Bridge متنكّرة في هيئة برنامج مراقبة شبكات، للإبقاء على وصول خفي إلى الشبكات المخترقة وتجنب الكشف.

- توصف Webworm بأنها جهة تهديد مرتبطة بالصين.
- يُشتبه في استخدامها نسخة مخصصة من أداة SoftEther VPN Bridge مفتوحة المصدر.
- تهدف التعديلات على ما يبدو إلى إزالة البصمات التي تتعرف عليها أدوات الأمن.
- تُقدَّم الأداة على أنها برنامج لمراقبة الشبكات.
- الغاية هي الوصول عن بُعد بشكل خفي إلى الشبكات المخترقة.

ما الذي ورد في التقرير

يُشتبه في أن Webworm، وهي جهة تهديد توصف بأنها مرتبطة بالصين، تستخدم نسخة مخصصة من أداة **SoftEther VPN Bridge** مفتوحة المصدر. وبحسب التقرير، أزالت النسخة المعدّلة البصمات التي تعتمد عليها أدوات الكشف عادة، وتوظف عدة حيل لإخفاء نفسها عن أدوات الأمن.

كما يُذكر أن الأداة تُقدَّم على أنها برنامج لمراقبة الشبكات، بهدف إقامة وصول خفي عن بُعد إلى شبكات سبق اختراقها.

لماذا يهم ذلك

تُعد SoftEther أداة VPN مشروعة ومتاحة على نطاق واسع، لذا قد لا يكشف الاعتماد على التواقيع النسخة المعدّلة منها. وقد تمر عملية أو خدمة تبدو كمنتج مراقبة دون انتباه عند المراجعة السريعة. ويبقى الإسناد والتفاصيل التقنية الكاملة لدى المصدر الأصلي، والنشاط موصوف بأنه مشتبه به.

قراءة عملية لفرق الأمن

الدرس العملي أن وجود قدرة VPN أو نفق غير متوقعة على الخوادم يُعد نتيجة تستحق المعالجة أياً كان اسم البرنامج. والفحوص السلوكية، مثل الأنفاق الصادرة غير المعتادة والخدمات غير المعتمدة وأدوات المراقبة غير الموجودة في سجل الأصول، أكثر موثوقية من مطابقة الاسم أو التوقيع لهذا النوع من الأدوات.

ما يجب فعله الآن

1. البحث في الخوادم ونقاط النهاية عن مكونات SoftEther، بما في ذلك الملفات التنفيذية والخدمات المعاد تسميتها والمقدَّمة كأدوات مراقبة.
2. مطابقة كل أداة مراقبة أو وصول عن بُعد مثبتة مع سجل الأصول والبرمجيات المعتمد.
3. إضافة قواعد كشف للأنفاق VPN غير المتوقعة والاتصالات الصادرة طويلة الأمد وغير المعتادة من الخوادم.
4. تقييد حركة البيانات الصادرة من الخوادم إلى وجهات معتمدة ومراجعة سجلاتها.
5. تطبيق قوائم السماح بالتطبيقات على الخوادم الحساسة لمنع تشغيل أدوات الشبكة غير المعتمدة.
6. عند العثور على تطابق، التصعيد عبر مسار الاستجابة للحوادث والالتزام بمتطلبات الإبلاغ لدى الهيئة الوطنية للأمن السيبراني.