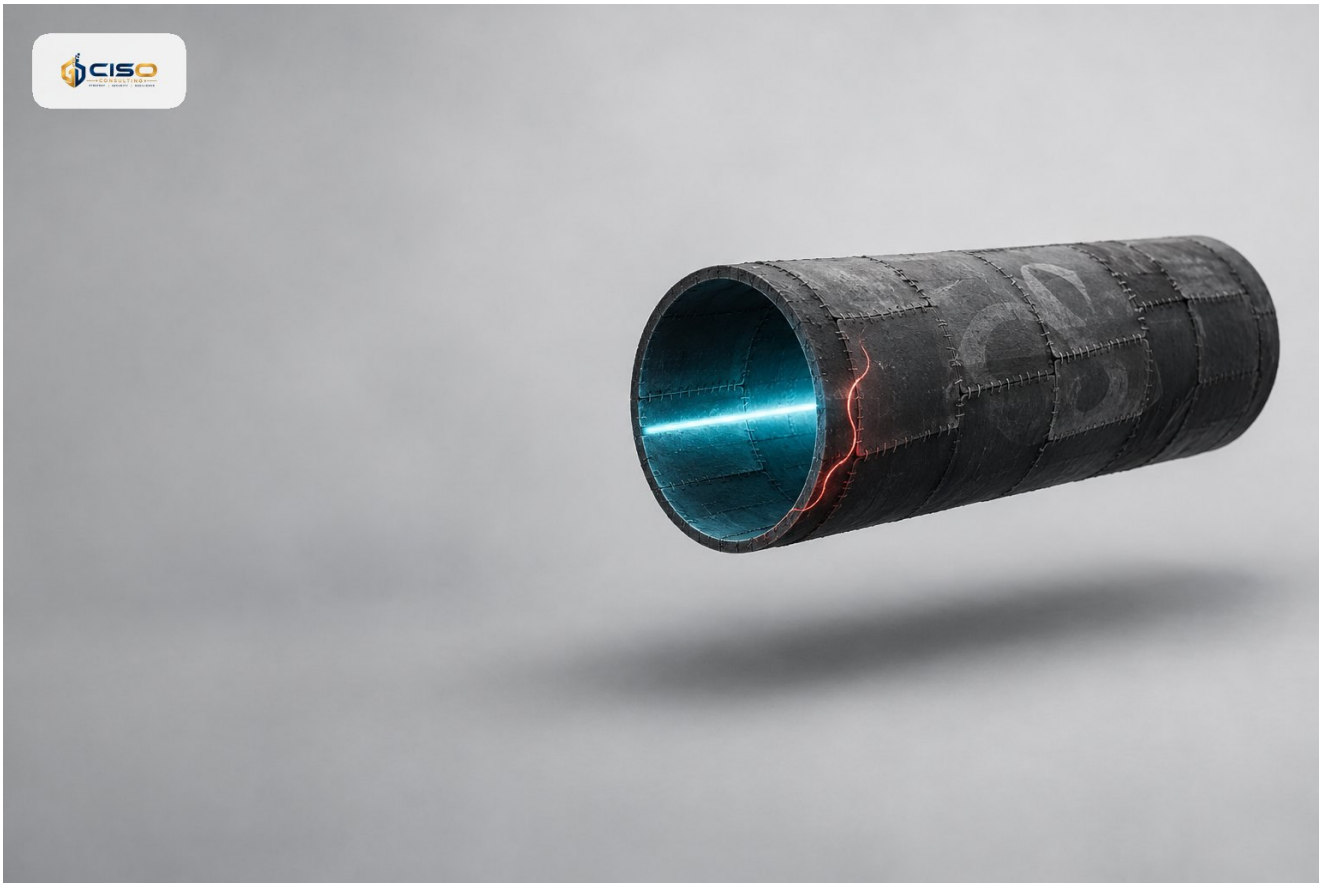
# مجموعة Webworm تستخدم نسخة معدّلة من SoftEther VPN للتخفي عن فرق الدفاع



أعادت مجموعة التجسس Webworm المرتبطة بالصين بناء برنامج SoftEther VPN مفتوح المصدر من شيفرته، وأزالت منه الآثار التي تكشفه عادةً. يُنصح بمراجعة آليات رصد برمجيات VPN غير المصرّح بها.

- توصَف Webworm بأنها مجموعة تجسس مرتبطة بالصين.
- أعادت المجموعة بناء برنامج SoftEther VPN المفتوح المصدر من شيفرته المصدرية.
- النسخة المعدّلة تُزيل الآثار التي تكشفه عادةً أمام فرق الدفاع.
- وعليه قد لا تلتقطها وسائل الرصد المعتمدة على الخصائص الافتراضية المعروفة للبرنامج.

## ما الذي ورد في التقرير

يفيد موقع Dark Reading بأن مجموعة التجسس Webworm، المرتبطة بالصين، تستخدم نسخة معدّلة من SoftEther VPN. فبدلًا من نشر الإصدار القياسي، قامت المجموعة بتجميع البرنامج مفتوح المصدر بنفسها انطلاقاً من شيفرته المصدرية.

وأتاح هذا الأسلوب إزالة الآثار التي تكشف البرنامج عادةً، وهي السمات التي يعتمد عليها المدافعون للتعرف على الأداة داخل الشبكة.

## أهمية الأمر

SoftEther برنامج مشروع ومتاح مجاناً. وحين يعيد المهاجم تجميعه ويحذف سماته المميّزة، قد لا تنطبق قواعد الرصد المبنية على النسخة المعتادة. وبذلك يمتزج البرنامج مع النشاط الاعتيادي للشبكة ويمنح المهاجم قناة أكثر هدوءاً للدخول إلى البيئة.

ولا يذكر ملخص المصدر ضحايا أو مناطق أو مؤشرات تقنية، لذا لا ينبغي الجزم بتأثر جهة ما أو عدم تأثرها استناداً إلى هذا التقرير وحده.

## نظرة عملية

الدرس هنا لا يخص أداة بعينها؛ فالاعتماد على التوقيعات المعروفة لبرمجيات الوصول عن بُعد وحدها يضعف الحماية أمام النسخ المعدّلة. أما المراقبة السلوكية، وجرد دقيق لأدوات الوصول عن بُعد المعتمدة، وضوابط الاتصال الصادر، فتوفر تغطية أوسع. ويمكن لفرق الأمن في الجهات المنظَّمة اعتبار هذا التقرير دافعاً لاختبار قدرتها على رصد خدمة VPN غير معتمدة.

## ما يجب فعله الآن

1. الاحتفاظ بجرد لأدوات الوصول عن بُعد وVPN المعتمدة، والتنبيه على أي أداة خارجه.
2. إضافة قواعد رصد سلوكية للأنفاق الشبيهة بـVPN غير المتوقعة والاتصالات الصادرة غير المعتادة، وعدم الاكتفاء بالتوقيعات.
3. مراجعة ضوابط تصفية الاتصال الصادر لتحديد الأجهزة المسموح لها بفتح أنفاق خارجية.
4. البحث عن نشاط مرتبط بـSoftEther، بما في ذلك النسخ المعاد تجميعها أو المعاد تسميتها، على الخوادم والأجهزة الطرفية.
5. اختبار قدرة منظومة المراقبة على كشف خدمة VPN غير معتمدة ومعالجة الثغرات التي تظهر.