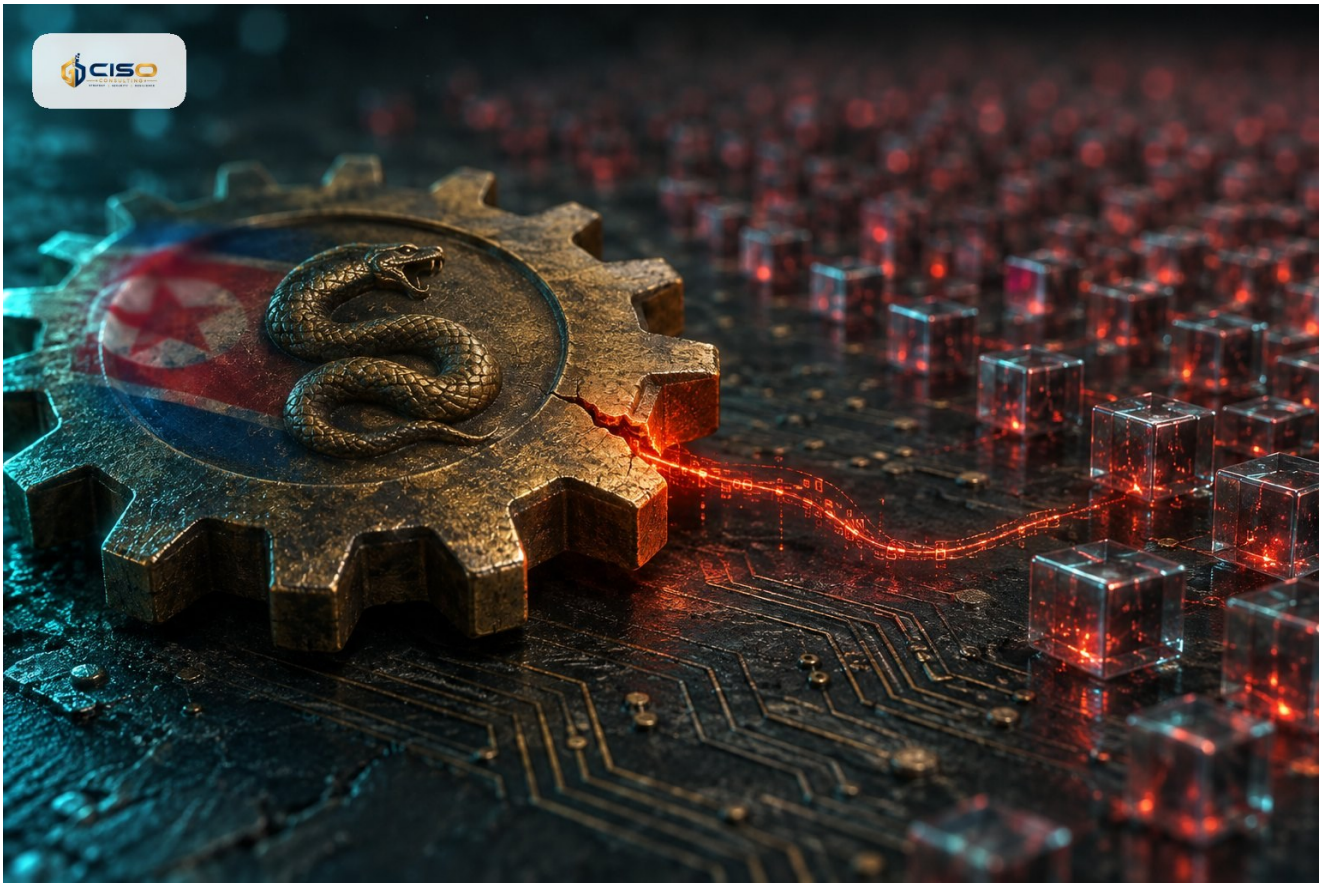
حملة PolinRider تزرع محمّلات بايثون في أكثر من 7,600 مستودع على GitHub



تفيد SafeDep بأن حملة PolinRider المرتبطة بكوريا الشمالية زرعت محمّل بايثون في أكثر من 7,600 مستودع على GitHub، وربما منذ فبراير 2025.

- ترتبط حملة PolinRider بكوريا الشمالية وقد طالت أكثر من 7,600 مستودع على GitHub.
- يوضع المحمّل الخبيث في حزمة utils صغيرة أو في الملف conftest.py.
- يعمل المحمّل عند استيراد بايثون للملف.
- يشير تقرير SafeDep إلى أن النشاط ربما بدأ منذ فبراير 2025.

ما الذي ورد في التقرير

تصف The Hacker News، نقلًا عن تقرير نشرته SafeDep هذا الأسبوع، حملة باسم **PolinRider** تُنسب إلى جهات

مرتبطة بكوريا الشمالية. وتفيد التقارير بأنها زرعت محمّل بايثون في مستودعات على GitHub، وأن أكثر من 7,600 مستودع قد تأثر.

وتذكر SafeDep أن المحمّل يختبئ في حزمة utils صغيرة أو في الملف conftest.py، ويبدأ عمله عندما تستورد بايثون هذا الملف. والمقتطف المتاح من المصدر مبتور، لذلك لا تتوافر هنا تفاصيل عمّا يجلبه المحمّل أو يسلّمه.

كما توجد دلائل على أن النشاط ربما بدأ منذ فبراير 2025.

أهمية الأمر

تعتمد هذه الطريقة على شيفرة يستوردها المطورون وخطوط البناء بصورة اعتيادية. فالملفات المساعدة وملفات إعداد الاختبارات نادراً ما تخضع لمراجعة دقيقة، ما قد يتيح تنفيذ شيفرة خبيثة على أجهزة المطورين أو أنظمة التكامل المستمر دون مؤشر واضح.

على الجهات التي تعتمد على شيفرة بايثون مفتوحة المصدر أو تستنسخ مستودعات خارجية وتختبرها أن تعدّ ذلك مخاطر سلسلة توريد تستحق الفحص، دون افتراض أنها متأثرة.

النهج المقترح

راجعوا ما تسحبه فرقكم من المستودعات العامة، وابحثوا عن تغييرات غير متوقعة في الملفات المساعدة وملفات إعداد الاختبارات، وارجعوا إلى تقرير SafeDep الكامل للاطلاع على مؤشرات الاختراق متى أمكن.

ما يجب فعله الآن

1. احصروا مستودعات GitHub العامة التي يستنسخها مطوروكم وخطوط التكامل المستمر أو يعتمدون عليها.
2. افحصوا شيفرة بايثون الداخلية والمستنسخة بحثاً عن محتوى غير متوقع في حزم utils وملفات conftest.py.
3. شغّلوا المستودعات غير الموثوقة واختباراتها في بيئات معزولة لا تملك وصولًا إلى بيانات اعتماد الإنتاج.
4. احصلوا على تقرير SafeDep الكامل وطابقوا مؤشراته مع مستودعاتكم وأجهزتكم.
5. وجّهوا فرق التطوير إلى مراجعة الشيفرة الخارجية قبل استيرادها أو اختبارها.