اختراق حزمة Microsoft Agent Framework على PyPI لسرقة بيانات الاعتماد



اخترق مهاجمون حزمة Microsoft Agent Framework الرسمية على PyPI ونشروا نسختين خبيثتين مصممتين لسرقة بيانات الاعتماد السحابية ومعلومات حساسة من أجهزة المطورين.

- تعرضت حزمة Microsoft Agent Framework الرسمية على PyPI للاختراق.
- نُشرت نسختان خبيثتان من الحزمة.
- صُمم الكود الخبيث لسرقة بيانات الاعتماد السحابية ومعلومات حساسة أخرى.
- الأهداف هي أجهزة المطورين.

ما الذي حدث

وفق ما نشره موقع BleepingComputer، اخترق مهاجمون حزمة Microsoft Agent Framework الرسمية المكتوبة

بلغة Python على مستودع PyPI، ونشروا نسختين خبيثتين منها صُمّمتا لجمع بيانات الاعتماد السحابية ومعلومات حساسة أخرى من أجهزة المطورين الذين ثبّتوهما.

لماذا يهم ذلك

تُوزَّع الحزمة باسم Microsoft عبر قناة رسمية، وقد تُثبَّت أو تُحدَّث دون تدقيق إضافي. وهذا مثال على مخاطر سلسلة توريد البرمجيات، إذ تصبح مكتبة موثوقة وسيلةً للهجوم. كما أن سرقة بيانات الاعتماد السحابية قد تمنح المهاجم وصولًا إلى بيئات سحابية تتجاوز جهاز المطور نفسه.

لا يحدد المقتطف المتاح لدينا أرقام النسخ المتأثرة ولا النطاق الزمني بدقة ولا السلوك التقني الكامل للبرمجية الخبيثة، لذا ينبغي الرجوع إلى التقرير الأصلي وإلى أي إشعار من Microsoft أو PyPI قبل إجراء فحوص محددة للنسخ.

الخطوات التالية

على الجهات التي تستخدم Python في تطوير حلول الذكاء الاصطناعي والوكلاء التحقق من وجود الحزمة في مشاريعها وخطوط البناء وأجهزة المطورين، ومن تثبيت أي من النسختين الخبيثتين. وفي حال ثبت ذلك، تُعامل البيئة المتأثرة على أنها مكشوفة، وتُدوَّر بيانات الاعتماد السحابية التي يمكن الوصول إليها منها.

ما يجب فعله الآن

1. البحث في المستودعات وخطوط البناء وأجهزة المطورين عن حزمة Microsoft Agent Framework وتحديد النسخ المثبتة.
2. مراجعة التقرير الأصلي وإشعارات Microsoft أو PyPI لتأكيد النسخ الخبيثة.
3. عند تثبيت نسخة خبيثة، عزل الجهاز وتدوير جميع بيانات الاعتماد والرموز والمفاتيح السحابية التي يمكن الوصول إليها منه.
4. مراجعة سجلات التدقيق السحابية بحثاً عن نشاط غير معتاد مرتبط بالبيانات المكشوفة.
5. تثبيت إصدارات الاعتماديات وتمرير تثبيت الحزم عبر مستودع داخلي موثوق أو عملية موافقة.