التلاعب بخوادم تحديث AOMEI Backupper لتسليم باب خلفي



عدّل مهاجمون ملفات على خوادم تحديث AOMEI لفترات قصيرة بين مايو ويوليو 2026، فتلقّت نسخ AOMEI Backupper التي فحصت التحديثات خلالها بابًا خلفيًا.

- غيّر المهاجمون ملفات على خوادم التحديث الخاصة بالمورّد نفسه.
- استمرت كل نافذة تلاعب نحو خمس إلى عشر دقائق، وتكررت بين مايو ويوليو 2026.
- أي نسخة من AOMEI Backupper على ويندوز فحصت التحديثات خلال إحدى النوافذ نزّلت بابًا خلفيًا وشغّلته.
- يذكر المصدر مجموعة Google Threat Intelligence وMandiant وفريق Threat Analysis التابع لـManageEngine في سياق هذه النتائج.

ما الذي أُبلغ عنه

وفق ما نشره موقع The Hacker News، عدّل مهاجمون مرارًا الملفات التي يجلبها AOMEI Backupper من خوادم التحديث التابعة للمورّد نفسه. وكانت كل عملية تعديل تدوم من خمس إلى عشر دقائق فقط، وجرت بين مايو ويوليو 2026.

والنتيجة أن أي نسخة من برنامج النسخ الاحتياطي على ويندوز فحصت وجود تحديث خلال إحدى هذه النوافذ القصيرة كانت تنزّل بابًا خلفيًا وتشغّله. ويشير المصدر إلى مجموعة Google Threat Intelligence وMandiant وفريق Threat Analysis التابع لـManageEngine في سياق هذه النتائج.

لماذا يهم ذلك

جاء التسليم عبر آلية التحديث المعتادة للمنتج، أي من مصدر يثق به البرنامج أصلاً. وتعمل أدوات النسخ الاحتياطي عادةً بصلاحيات مرتفعة وتتعامل مع بيانات حساسة، فيغدو اختراق أي نسخة منها مصدر قلق كبير. كما أن قصر النوافذ يعني أن التعرض يعتمد على توقيت فحص كل جهاز للتحديثات، فغياب الأعراض الظاهرة لا يعني السلامة.

ولا يتضمن المقتطف مؤشرات اختراق ولا أرقام الإصدارات المتأثرة ولا إصلاحًا من المورّد، لذا ينبغي الرجوع إلى التقرير الكامل وإرشادات المورّد.

الخطوات التالية

على المنشآت أولاً تحديد ما إذا كان AOMEI Backupper مثبتًا في بيئتها، بما في ذلك الخوادم والأجهزة المشتراة خارج المشتريات المركزية. وحيث وُجد، تُراجع أنشطة التحديث بين مايو ويوليو 2026، ويُعامل أي جهاز فحص التحديثات في تلك الفترة على أنه متأثر محتمل إلى أن يثبت العكس.

ما يجب فعله الآن

1. حصر جميع الأجهزة التي يعمل عليها AOMEI Backupper، بما فيها الخوادم والأجهزة غير المُدارة.
2. مراجعة سجلات التحديث والشبكة للفترة من مايو إلى يوليو 2026 لتحديد الأجهزة التي اتصلت بخوادم التحديث.
3. اعتبار الأجهزة التي فحصت التحديثات في تلك الفترة مخترقة محتملاً والتحقيق فيها قبل الوثوق بنسخها الاحتياطية.
4. الاطلاع على إرشادات المورّد والباحثين لمعرفة مؤشرات الاختراق والإصدارات المصححة.
5. النظر في تعطيل التحديث التلقائي لأدوات النسخ الاحتياطي إلى حين التحقق من التحديثات.