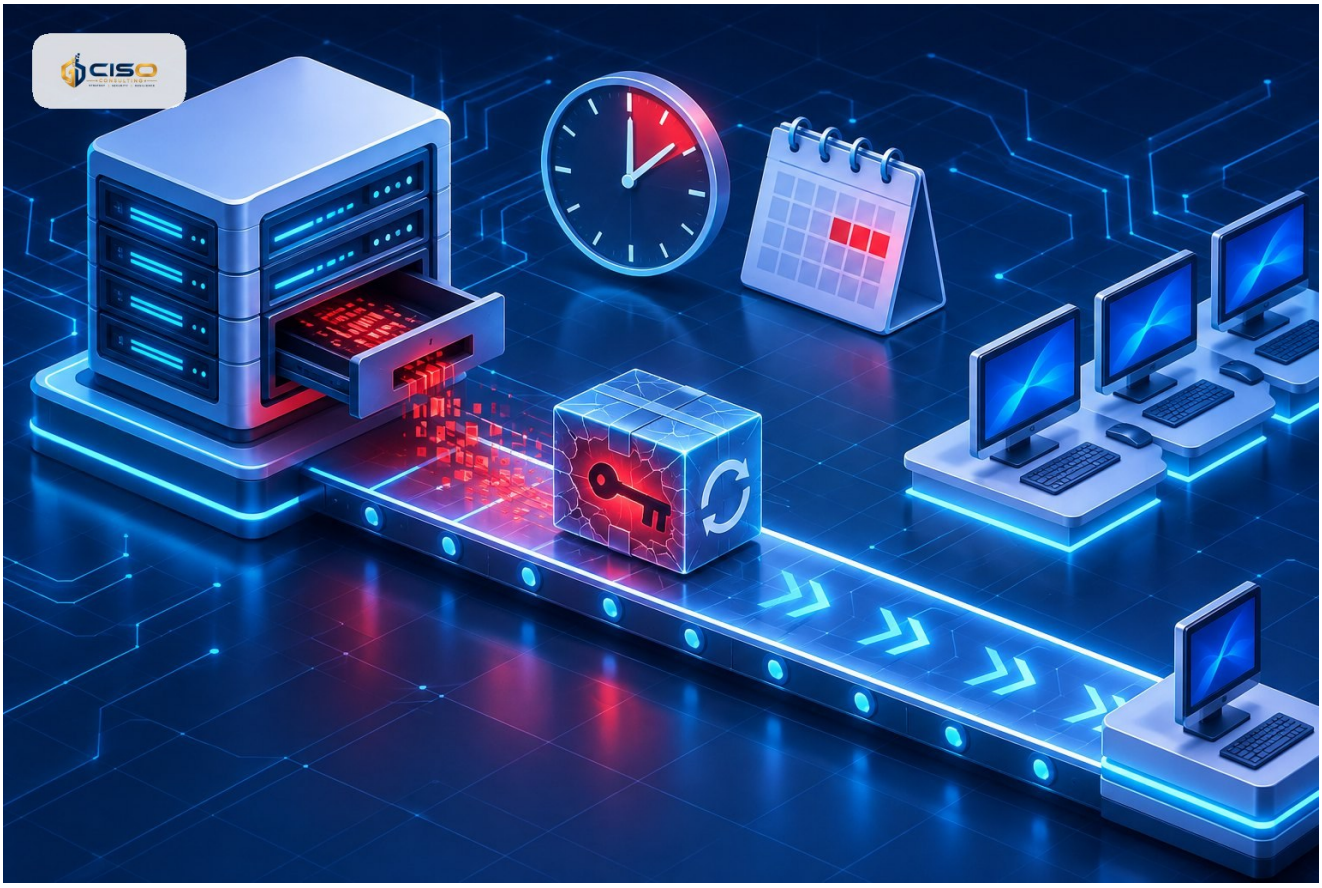
التلاعب لفترات وجيزة بخوادم تحديث AOMEI Backupper لتوزيع باب خلفي



عدّل مهاجمون ملفات على خوادم التحديث التابعة للجهة المطورة لبرنامج AOMEI Backupper في فترات قصيرة بين مايو ويوليو 2026، فقد تنزّل النسخ التي فحصت التحديثات خلالها بابًا خلفيًا وتشغّله.

- غيّر المهاجمون ملفات على خوادم التحديث الرسمية للجهة المطورة، لا على موقع طرف ثالث.
- استمرت كل نافذة تلاعب نحو خمس إلى عشر دقائق، وتكررت بين مايو ويوليو 2026.
- أي نسخة على Windows فحصت التحديثات خلال إحدى النوافذ قد تنزّل بابًا خلفيًا وتشغّله.
- يذكر المصدر مجموعة Google Threat Intelligence Group وشركة Mandiant وفريق Threat Analysis التابع لـ ManageEngine ضمن الجهات المرتبطة بالتقرير.

ما الذي ورد في التقرير

وفق موقع The Hacker News، عدّل مهاجمون مرارًا الملفات التي يجلبها برنامج النسخ الاحتياطي AOMEI Backupper لنظام Windows من خوادم التحديث التابعة للجهة المطورة نفسها. جرى التعديل في نوافذ قصيرة تراوحت بين خمس وعشر دقائق تقريبًا، وتكررت بين مايو ويوليو 2026.

وأي نسخة فحصت وجود تحديث خلال إحدى هذه النوافذ كانت ستنزّل بابًا خلفيًا وتشغّله بدلاً من تحديث سليم. وينسب التقرير النتائج إلى Google Threat Intelligence Group وMandiant وفريق Threat Analysis التابع لـ ManageEngine.

أهمية الأمر

تعمل برامج النسخ الاحتياطي عادةً بصلاحيات مرتفعة وتصل إلى بيانات واسعة، لذا يمثل اختراق قناة التحديث مدخلاً خطيرًا إلى البيئة. وبما أن النوافذ كانت قصيرة، فقد تتعرض جهة ما دون أي مؤشر واضح، وغياب التنبيهات لا يعني السلامة.

لا يتضمن المقتطف مؤشرات فنية ولا اسم الباب الخلفي ولا أرقام الإصدارات المتأثرة، ويُستحسن طلب هذه التفاصيل من الجهة المطورة ومن الباحثين.

النهج المقترح

ينبغي للمؤسسات أولاً تحديد ما إذا كان AOMEI Backupper موجودًا في بيئتها، بما في ذلك محطات المسؤولين والخوادم غير المسجلة مركزيًا. وإن وُجد فليُراجع حدوث فحوص تحديث تلقائية بين مايو ويوليو 2026، وتُعامل تلك الأجهزة على أنها متأثرة محتملاً إلى حين التحقق.

ما يجب فعله الآن

1. حصر جميع الأجهزة التي يعمل عليها AOMEI Backupper، بما فيها المحطات والخوادم غير المُدارة.
2. تحديد الأجهزة التي ربما أجرت فحص تحديث بين مايو ويوليو 2026 ومعاملتها كأجهزة مشتبه بها حتى التحقق.
3. التواصل مع الجهة المطورة ومراجعة تقارير الباحثين للحصول على مؤشرات الاختراق، ثم البحث عنها في سجلات الأجهزة والشبكة.
4. إيقاف التحديث التلقائي للبرنامج إلى أن تؤكد الجهة المطورة سلامة قناة التحديث.
5. التحقق من سلامة النسخ الاحتياطية الصادرة عن الأجهزة المشتبه بها وحفظها بمعزل عن بيانات اعتماد بيئة الإنتاج.