

إساءة استخدام خوادم تحديث AOMEI Backupper لتوزيع برمجيات خبيثة في هجمات سلسلة التوريد



عدّل مهاجمون ملفات الإعداد على خوادم AOMEI لفترات قصيرة بين أبريل ويوليو 2026 لنشر CROSSROAD و SHINYROAD لدى مستخدمي AOMEI Backupper. ينبغي للجهات المستخدمة للبرنامج البحث عن أي اختراق.

- وقعت الهجمات بين أبريل ويوليو 2026 عبر نظامي التحديث والإشعارات في AOMEI Backupper، وهو تطبيق ويندوز للنسخ الاحتياطي ونسخ الأقراص.
- عدّل ملفا الإعداد down_html.ini و Notifycfg.ini لفترات وجيزة، كما غُيّر مجموع التحقق المتوقع ليجتاز الأرشيف الخبيث فحص التحقق.
- حُدثت ثلاث نوافذ تعرّض مدتها بين 5 و10 دقائق: 28 مايو و16 يوليو و20 يوليو.
- شملت البرمجيات CROSSROAD للتحميل و SHINYROAD كباب خلفي يستغل مكونات Radmin، ويُنسب النشاط إلى الجهة UNC7017.

- بحسب ManageEngine، لا يزال إصلاح الخادام البرمجيات الخبيثة المثبتة مسبقاً على الأجهزة.

ما الذي حدث

أفاد باحثو مختبر ManageEngine لتحليل التهديدات، بالتعاون مع مجموعة استخبارات التهديدات في Google وشركة Mandiant، بأن مهاجمين اخترقوا الخوادم التي تستخدمها AOMEI لخدمة برنامج Backupper. ولم يستبدل المهاجمون الملفات بشكل دائم، بل عدّلوا ملفي إعداد لفترة وجيزة ثم أعادوهما إلى حالتهما خلال دقائق، ما صعب الكشف.

يحدد أحد الملفين مصدر تنزيل حزم التحديث، بينما ينظم الآخر الإشعارات ويمكنه تشغيل محتوى على الجهاز. وجّه المهاجمون البرنامج إلى أرشيف ZIP خبيث، وغيّروا مجموع التحقق المتوقع ليجتاز الفحص، واستخدموا آلية الإشعارات لتنفيذ الحمولة دون تدخل المستخدم.

الأثر

شملت البرمجيات الخبيثة CROSSROAD الذي يجمع معلومات عن الجهاز ويحقّل مكونات إضافية ويثبت نفسه عبر مهمة مجدولة، وSHINYROAD وهو باب خلفي يستخدم مكونات Radmin الشرعية للاتصال بخادم يتحكم فيه المهاجم. وفي 20 يوليو رصدت Google أيضاً محاولة للحصول على تجزئات NTLM في ويندوز عبر مورد WebDAV.

وُجدت جهات متأثرة في دول عدة منها الولايات المتحدة وأستراليا والهند وسنغافورة وإسبانيا وسويسرا، في قطاعات خدمات تقنية المعلومات والاتصالات والتعليم العالي. ووصفت Google الهجمات بأنها انتهازية، وقد تكون جهات أخرى تحققت من التحديثات خلال النوافذ القصيرة متأثرة أيضاً.

موقف الشركة

تقول AOMEI إنها رقت خوادمها وتحققت منها وإن مديرها التقني يقود التحقيق، لكنها لم تؤكد كيفية وصول المهاجمين ولا اكتمال المعالجة. وتشدد ManageEngine على أن تأمين الخوادم يوقف الإصابات الجديدة لكنه لا ينظف الأجهزة التي تلقت البرمجيات الخبيثة.

ما يجب فعله الآن

1. حصر جميع الأجهزة التي يعمل عليها AOMEI Backupper، بما في ذلك التثبيتات غير المدارة أو على مستوى الإدارات.
2. مراجعة مؤشرات الاختراق التي نشرتها Google وManageEngine والبحث عن المهام المجدولة المشبوهة وملفات تنفيذية غير متوقعة في مجلدات AOMEI وتثبيتات Radmin غير المعتمدة.
3. فحص سجلات الوكيل وDNS بحثاً عن اتصالات بعنوان IP وأسماء المضيفين المبلغ عنها منذ أبريل 2026.
4. عند اكتشاف إصابة: عزل الجهاز وحفظ الأدلة وإعادة تعيين بيانات الاعتماد المكشوفة عليه واعتبار تجزئات NTLM محتمل التقاطها.
5. النظر في إيقاف التحديث التلقائي والإشعارات لهذا المنتج حتى تنشر الشركة نتائج تحقيقها، وإدراج قنوات التحديث لدى الأطراف الثالثة في مراجعات مخاطر الموردين.