اكتشاف تلاعب بمثبّتات Q-Dir وDesktopOK على موقع SoftwareOK الرسمي



أفاد باحثون بهجوم على سلسلة التوريد عُدّلت فيه ملفات تثبيت Q-Dir وDesktopOK على موقع SoftwareOK الرسمي لنشر برمجية وصول عن بُعد، ومنها عبر التحديثات.

- جرى التلاعب بملفات تثبيت Q-Dir وDesktopOK الموزعة عبر موقع SoftwareOK الرسمي.
- تصف العناوين الحمولة الخبيثة بأنها برمجية وصول عن بُعد.
- ظهرت الملفات الخبيثة عند التنزيل المباشر من الصفحة الرسمية وكذلك أثناء تحديث النسخ المثبتة مسبقاً.
- لا يذكر المقتطف المتاح تواريخ أو أسماء برمجيات خبيثة أو إصدارات متأثرة.

كشف باحثون عن هجوم على سلسلة التوريد البرمجية يطال أداتين لنظام Windows هما Q-Dir وDesktopOK. فقد جرى التلاعب بملفات التثبيت الموزعة عبر موقع SoftwareOK الرسمي، والهدف المعلن هو إيصال برمجية وصول

عن بُعد.

ما هو معروف

وفق التقرير، لم تقتصر الملفات الخبيثة على التنزيلات الجديدة من صفحة التنزيل الرسمية، بل ظهرت أيضاً أثناء عملية تحديث نسخ سبق للمستخدمين تثبيتها. ويعني ذلك أن الثقة بالمصدر الرسمي أو الاعتماد على التحديث المدمج لم يكونا كافيين لتفادي المشكلة.

لا يوضح المقتطف المتاح لنا توقيت النشاط ولا الإصدارات المتأثرة ولا عائلة البرمجية الخبيثة المستخدمة. ولذلك ينبغي انتظار التفاصيل التقنية الكاملة قبل الجزم بمؤشرات اختراق محددة.

أهمية الخبر

كثيراً ما يثبّت المسؤولون والموظفون أدوات صغيرة كهذه خارج مسار الشراء الرسمي، فلا تظهر في سجلات البرمجيات. كما أن مثبّتاً مخترقاً من مورد شرعي يتجاوز الحذر المعتاد تجاه المصادر المجهولة، وتمنح برمجية الوصول عن بُعد المهاجم موطئ قدم داخل الشبكة.

الخطوات التالية

يُنصح باستغلال الخبر للتحقق من وجود الأداتين في بيئتكم، ومراجعة آلية اعتماد هذه الأدوات وتحديثها، والتأكد من أن مراقبة الأجهزة الطرفية قادرة على رصد سلوك الوصول عن بُعد غير المتوقع.

ما يجب فعله الآن

1. البحث في الأجهزة وسجلات البرمجيات عن Q-Dir وDesktopOK، بما فيها النسخ التي ثبّتها المستخدمون بأنفسهم.
2. تعليق تثبيت هذه الأدوات أو تحديثها إلى حين صدور إرشادات واضحة من المورد أو الباحثين، والتحقق من المثبّتات بالرجوع إلى التقرير التقني الكامل.
3. فحص الأجهزة التي ثُبّتت عليها إحدى الأداتين أو حُدّثت مؤخراً بحثاً عن جلسات وصول عن بُعد أو اتصالات صادرة غير متوقعة.
4. إخضاع الأدوات المساعدة لمسار اعتماد وقائمة سماح، حتى لو كان مصدرها موقع المورد الرسمي.
5. التأكد من أن حلول رصد الأجهزة الطرفية وسجلاتها تغطي أدوات الوصول عن بُعد، وإطلاع مركز العمليات الأمنية على هذا التقرير.