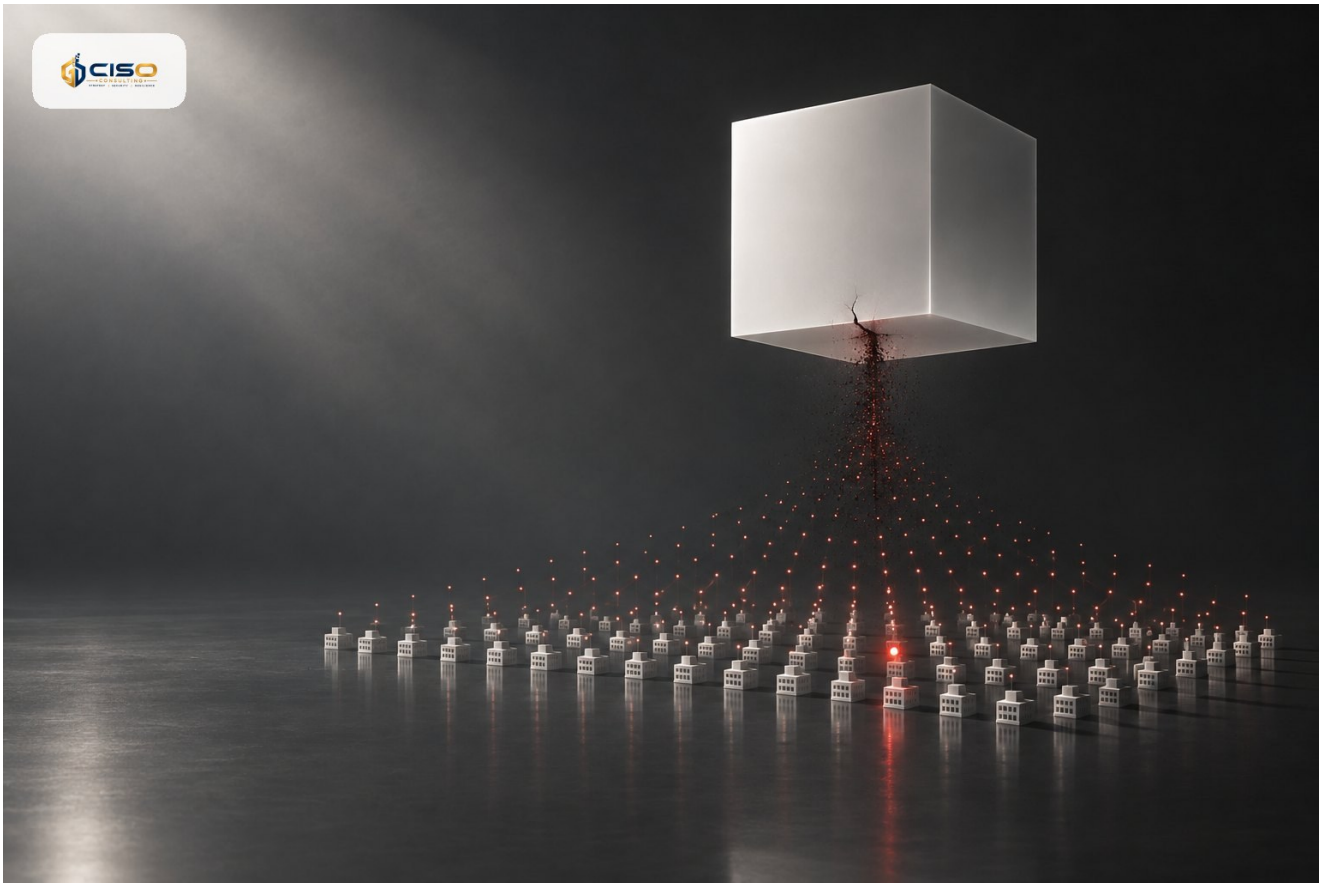
برمجيات خبيثة مرتبطة بمنصة Optimizely تعرّض زوار مواقع 178 جهة على الأقل



عرّضت 178 جهة على الأقل، بينها علامات تجارية كبرى، زوار مواقعها لبرمجيات خبيثة دون علمها عبر منصة طرف ثالث هي Optimizely، في مثال على اتساع سطح الهجوم عبر الموردين.

- تأثرت 178 جهة على الأقل، من بينها عدة علامات تجارية كبرى.
- تعرّض زوار المواقع لبرمجيات خبيثة وُصفت بأنها متعددة الرؤوس على غرار الهيدرا.
- لم تكن الجهات على علم بذلك، وجاء التعرض عبر منصة طرف ثالث هي Optimizely.
- تُعرض الحادثة بوصفها مثالًا على مخاطر الموردين من الأطراف الثالثة.

ما الذي ورد في التقرير

ذكر موقع Dark Reading أن 178 جهة على الأقل، من بينها عدة علامات تجارية كبرى، عرّضت زوار مواقعها

لبرمجيات خبيثة دون علمها. ولم يكن مصدر التعرض أنظمة هذه الجهات نفسها، بل منصة طرف ثالث هي Optimizely. ووُصفت البرمجيات بأنها متعددة الرؤوس على غرار الهيدرا.

المقال المصدر موجز، ولا يوضح الآلية التقنية ولا الإطار الزمني ولا أسماء الجهات المتأثرة ولا عدد الزوار الذين وصلت إليهم البرمجيات. لذلك لم نفترض أياً من هذه التفاصيل.

أهمية الأمر

الدرس الأساسي أن المواقع العامة للمؤسسة قد تصبح قناة لنشر البرمجيات الخبيثة حتى لو كانت بنيتها الداخلية محمية جيداً. فالجهات التي تعتمد على منصات خارجية في أصولها الرقمية ترث جزءاً من مخاطر هذه المنصات، ويقع الضرر على عملائها.

وبالنسبة للجهات المنظمة في المملكة، يذكّر ذلك بأن مخاطر الأطراف الثالثة لا تقتصر على معالجي البيانات والخدمات المُسندة، بل تشمل الخدمات التي تحدد ما يحمّله متصفح الزائر.

الخطوات التالية

لا يشير المصدر إلى تأثر جهات سعودية. والخطوة المناسبة هي التحقق من موقفكم: حصر المنصات الخارجية التي تعتمد عليها مواقعكم، ومطالبة مزوديها بما توصلوا إليه، والتأكد من قدرتكم على الكشف والاستجابة بسرعة إذا وصلت مشكلة من جهة المورد إلى عملائكم.

ما يجب فعله الآن

1. حصر جميع منصات الأطراف الثالثة والنصوص البرمجية التي تحمّلها مواقعكم وبوابتكم العامة، وتحديد مالك لكل منها.
2. مطالبة الموردين المعنيين، ومنهم Optimizely إن كنتم تستخدمونها، بالإفادة كتابياً عما إذا تأثرت أصولكم.
3. مراجعة عقود الأطراف الثالثة للتأكد من التزامات الإبلاغ عن الحوادث وحق الحصول على ضمانات أمنية.
4. مراقبة المواقع العامة لرصد أي تغيير غير متوقع في المحتوى المحمّل، وتجهيز إجراء لتعطيل مكوّن المورد بسرعة.
5. إدراج اختراق المحتوى من جهة المورد ضمن تقييمات مخاطر الأطراف الثالثة وخطط الاستجابة، بما يتوافق مع متطلبات الأطراف الثالثة في ضوابط الهيئة الوطنية للأمن السيبراني (ECC).