هجوم يُشتبه أنه على سلسلة التوريد لدى Optimizely يُحمّل شيفرة JavaScript خبيثة على مواقع كبرى



أدى هجوم يُشتبه أنه على سلسلة التوريد لدى Optimizely إلى تحميل شيفرة JavaScript خبيثة على مواقع شهيرة منها Zoom وCNN وBBC وSalesforce وGitLab، وتستهدف الشيفرة بيانات العملات المشفرة والدفع وثغرات iOS.

- توصف الحادثة بأنها هجوم مشتبه على سلسلة التوريد يتعلق بـ Optimizely.
- جرى تحميل شيفرة JavaScript خبيثة على مواقع شهيرة عديدة.
- من المواقع المذكورة Zoom وCNN وFox News وBBC وSalesforce وGitLab.
- تهدف الشيفرة إلى سرقة العملات المشفرة ومعلومات الدفع.
- كما تحاول استغلال ثغرات في أجهزة iOS.

ما الذي ورد في التقرير

أفاد موقع BleepingComputer بوجود هجوم يُشتبه أنه على سلسلة التوريد يتعلق بشركة Optimizely، ونتج عنه تحميل شيفرة JavaScript خبيثة على مواقع معروفة عديدة، منها Zoom وCNN وFox News وBBC وSalesforce وGitLab.

ماذا تفعل الشيفرة

وفق التقرير، تعرّض زوار هذه المواقع لشيفرات مصممة لسرقة العملات المشفرة ومعلومات الدفع، ولاستغلال ثغرات في أجهزة iOS. ولا يتضمن المقتطف المتاح تفاصيل تقنية إضافية، لذا ينبغي التحقق من النطاق والجدول الزمني وحالة المعالجة لدى المورّد وفي التقرير الأصلي.

لماذا يهم ذلك

تبيّن الحادثة كيف يمكن لمورّد شيفرات خارجية أن يصبح قناة لإيصال البرمجيات الخبيثة عبر مواقع موثوقة. وتتحمل الجهات التي تحمّل شيفرات JavaScript خارجية في صفحاتها الموجهة للعملاء، خاصة صفحات الدفع وتسجيل الدخول، مخاطر المورّد حتى لو لم تتأثر أنظمتها.

وما دام الهجوم موصوفاً بأنه مشتبه، فقد تتغير التفاصيل مع تقدم التحقيق. والاستجابة المناسبة مراجعة هادئة قائمة على الأدلة لمدى اعتمادكم على الشيفرات الخارجية.

ما يجب فعله الآن

1. حصر جميع الشيفرات الخارجية، ومنها Optimizely، المحمّلة في مواقعكم وتطبيقاتكم العامة.
2. التحقق مما إذا كانت أصولكم الرقمية أو موردوكم نيابةً عنكم يستخدمون Optimizely.
3. مراجعة سجلات الويب والمراقبة بحثاً عن تغييرات غير متوقعة في الشيفرات أو نطاقات خارجية غير معروفة.
4. تطبيق سياسة Content Security Policy وضوابط سلامة الشيفرة للحد مما تستطيع الشيفرات الخارجية تنفيذه، خاصة في صفحات الدفع وتسجيل الدخول.
5. طلب حالة الحادثة من الموردين المعنيين، والاستعداد لإخطار العملاء والجهات التنظيمية إذا تعرض مستخدموكم للخطر.