هجوم يُشتبه أنه على سلسلة توريد Optimizely يحمّل شيفرة JavaScript خبيثة على مواقع علامات كبرى



أدى هجوم يُشتبه أنه استهدف سلسلة توريد Optimizely إلى تحميل شيفرة JavaScript خبيثة على مواقع شهيرة عدة، تسعى لسرقة العملات المشفرة وبيانات الدفع واستغلال ثغرات في أجهزة iOS.

- يوصف الحادث بأنه هجوم يُشتبه أنه استهدف سلسلة توريد Optimizely.
- جرى تحميل شيفرة JavaScript خبيثة على مواقع شهيرة عديدة.
- من المواقع المذكورة في التقرير: Zoom وCNN وFox News وBBC وSalesforce وGitLab.
- صُممت السكربتات لسرقة العملات المشفرة ومعلومات الدفع.
- كما تحاول استغلال ثغرات في أجهزة iOS.

ما الذي ورد في التقرير

يفيد موقع BleepingComputer بوجود هجوم يُشتبه أنه استهدف سلسلة توريد Optimizely، ما أدى إلى تقديم شيفرة JavaScript خبيثة على عدد من المواقع المعروفة، منها Zoom وCNN وFox News وBBC وSalesforce وGitLab.

ويصف التقرير هذه السكربتات بأنها مصممة لسرقة العملات المشفرة ومعلومات الدفع، ولاستغلال ثغرات في أجهزة iOS. ولا يتضمن المقتطف المتاح لنا تفاصيل إضافية عن آلية الهجوم أو تسلسله الزمني أو حجم الانكشاف، ولذلك ينبغي التحقق من هذه النقاط في التقرير الكامل وفي أي بيان من المزوّد.

لماذا يهم ذلك

يبيّن هذا الحادث كيف يمكن لسكربت أو خدمة من طرف ثالث أن يوصل شيفرة خبيثة إلى الزوار حتى لو لم تُخترق أنظمة مالك الموقع نفسها. وتتشارك المؤسسات التي تدمج شيفرات JavaScript خارجية في صفحاتها الموجهة للعملاء، ولا سيما صفحات الدفع أو الدخول، هذا الانكشاف.

النهج المقترح

لا حاجة للقلق المفرط، لكن مراجعة سريعة مبررة. حدّدوا ما إذا كانت Optimizely أو سكربتات مماثلة من أطراف ثالثة مستخدمة في أصولكم الرقمية، وتابعوا الإرشادات الرسمية من المزوّد، وتأكدوا من قدرتكم على رصد أي تغيير غير متوقع في السكربتات التي تحمّلها صفحاتكم.

ما يجب فعله الآن

1. حصر جميع السكربتات الخارجية المستضافة لدى أطراف ثالثة في المواقع والتطبيقات العامة، والتأكد مما إذا كانت Optimizely بينها.
2. متابعة النشرات الرسمية من Optimizely والجهات المتأثرة وتطبيق الخطوات الموصى بها.
3. مراجعة سجلات الويب وأنظمة المراقبة بحثاً عن مصادر سكربتات غير متوقعة أو تغيّر في محتواها على صفحات الدفع والدخول.
4. تطبيق ضوابط سلامة مثل Content Security Policy وSubresource Integrity حيثما أمكن، وتقليص الشيفرات الخارجية في الصفحات الحساسة.
5. عند تأكد الانكشاف، تقييم ما إذا تأثرت بيانات الدفع للعملاء واتباع إجراءات الاستجابة للحوادث والإبلاغ النظامي.