مكتب التحقيقات الفيدرالي يصادر سبعة نطاقات مرتبطة بأدوات Flax Typhoon لفحص البنية التحتية



أعلن مكتب التحقيقات الفيدرالي ووزارة العدل الأمريكية تعطيل أدوات مجموعة Flax Typhoon المرتبطة بالصين، عبر مصادرة نطاقات وحجب منصات استُخدمت لفحص البنية التحتية الحيوية الأمريكية واختراقها أحيانًا.

- أعلن مكتب التحقيقات الفيدرالي ووزارة العدل الأمريكية تعطيل أدوات تستخدمها Flax Typhoon، وهي مجموعة تهديد متقدم مستمر مرتبطة بالصين.
- صودرت سبعة نطاقات بحسب عنوان الخبر.
- حُجب الوصول إلى منصات استُخدمت لفحص البنية التحتية الحيوية الأمريكية واختراقها في بعض الحالات.
- المقتطف المتاح لا يذكر قائمة النطاقات ولا مؤشرات فنية.

أعلن مكتب التحقيقات الفيدرالي الأمريكي ووزارة العدل إجراءً ضد أدوات تستخدمها Flax Typhoon، وهي مجموعة تهديد متقدم مستمر يصفها المصدر بأنها مرتبطة بالصين.

ما الذي جرى

وفق التقرير، صادرت الجهات نطاقات، يحدد العنوان عددها بسبعة، وحجبت الوصول إلى منصات استخدمتها المجموعة. وقد استُخدمت هذه الأدوات لفحص البنية التحتية الحيوية الأمريكية، واختراقها في بعض الحالات. ينقطع المقتطف الذي اطلعنا عليه قبل ذكر قائمة النطاقات، ولذلك لا يمكننا تأكيد النطاقات أو المنصات المتأثرة.

الأهمية للجهات في المملكة

يتناول التقرير أهدافًا أمريكية ولا يشير إلى أي نشاط في المملكة. ومع ذلك فهو تذكير بأن مثل هذه الجهات تبدأ عادةً بفحص الأنظمة المكشوفة قبل أي اختراق. وقد ترغب مشغّلات البنية التحتية الحيوية والجهات المنظمة في المملكة في التأكد من معرفتها بأصولها المكشوفة ومراقبتها. كما أن تعطيل الأدوات لا يعني توقف نشاط المجموعة، إذ يمكن إعادة بناء بنيتها.

النهج المقترح

لا يحدد المصدر ثغرة أو مؤشرات بعينها، فلا يوجد ما يستدعي التصحيح بناءً عليه وحده. الخطوة العملية هي مراجعة الأصول المكشوفة وقدرات الرصد، وانتظار القائمة الكاملة للنطاقات المصادرة من الإصدارات الرسمية الأمريكية لمطابقتها مع السجلات.

ما يجب فعله الآن

1. مراجعة سجل الأصول المواجهة للإنترنت وإغلاق أو تقييد ما لا حاجة له.
2. التأكد من أن السجلات والتنبيهات تغطي عمليات الفحص والاستطلاع الواردة ضد الخدمات المكشوفة.
3. الحصول على القائمة الرسمية للنطاقات المصادرة من الجهات الأمريكية عند نشرها، والبحث عن أي تطابق في سجلات الوكيل وDNS وجدار الحماية.
4. التأكد من عزل بيئات التقنية التشغيلية عن تقنية المعلومات في البنية التحتية الحيوية ومن ضبط الوصول عن بُعد.
5. إحاطة فريق العمليات الأمنية والتأكد من مسار التصعيد إلى الجهة التنظيمية القطاعية المعنية.