ربط ثلاث مجموعات تجسس مرتبطة بالصين عبر منظومة البرمجيات الخبيثة Sparrow



رصدت Check Point Research ثلاث مجموعات نشاط تتشارك البنية التحتية وتشابهات في الشيفرة الخبيثة، استهدفت خلال العام الماضي قطاعات الاتصالات والحكومة والعسكرية والبحث والبنية التحتية الحرجة في أمريكا اللاتينية وآسيا وأوروبا.

- ثلاث مجموعات نشاط متمايزة تتشارك البنية التحتية وتتشابه في شيفرة البرمجيات الخبيثة.
- تتابعها Check Point Research، ومن أسمائها في المصدر SilentDelivery.
- تشمل الأهداف مزودي الاتصالات والجهات الحكومية والعسكرية والمؤسسات البحثية والبنية التحتية الحرجة.
- رُصد النشاط خلال العام الماضي في أمريكا اللاتينية وآسيا وأوروبا.
- يصف المصدر الحملات بأنها تجسسية مرتبطة بالصين ومتصلة عبر منظومة Sparrow.

وصفت Check Point Research ثلاث مجموعات نشاط تهديد منفصلة، تُتابَع كل منها على حدة، لكنها تتشارك البنية التحتية وتُظهر تشابهًا في شيفرة البرمجيات الخبيثة. ويربط المصدر بينها عبر منظومة برمجيات خبيثة مشتركة تُعرف باسم Sparrow، ويصف النشاط بأنه تجسس مرتبط بالصين.

ما الذي رُصد

خلال العام الماضي استهدفت هذه المجموعات مزودي خدمات الاتصالات والجهات الحكومية والكيانات العسكرية والمؤسسات البحثية والبنية التحتية الحرجة، وذلك في أمريكا اللاتينية وآسيا وأوروبا. ومن أسماء المجموعات الواردة في المصدر SilentDelivery، أما المقتطف المتاح فلا يذكر بقية الأسماء ولا تفاصيل تقنية مثل أساليب الوصول الأولي أو مؤشرات الاختراق أو المنتجات المتأثرة.

الأهمية للمملكة

تتقاطع القطاعات المستهدفة بدرجة كبيرة مع القطاعات الخاضعة للتنظيم في المملكة، وخصوصًا الاتصالات والجهات الحكومية والبنية التحتية الحرجة. ولا يذكر المصدر أي نشاط داخل المملكة أو الخليج، لذا فالأمر يتعلق بالوعي والجاهزية وليس بحادثة محلية مؤكدة. كما أن اشتراك المجموعات في البنية التحتية يعني أن معلومات التهديد عن مجموعة قد تساعد في كشف نشاط مرتبط بها.

ننصح بمراجعة منشور Check Point Research الكامل للاطلاع على المؤشرات والأساليب، واستخدامه في اختبار ترتيبات الكشف والاستجابة القائمة.

ما يجب فعله الآن

1. الحصول على تقرير Check Point Research الكامل واستخراج المؤشرات والأساليب المنشورة.
2. البحث في السجلات التاريخية وإجراء صيد للتهديدات عن المؤشرات المنشورة، مع إعطاء الأولوية لأنظمة الاتصالات والأنظمة المرتبطة بالجهات الحكومية والأنظمة الحرجة.
3. التأكد من أن مصادر معلومات التهديد لدى مركز العمليات الأمنية تغطي منظومة Sparrow والمجموعات المسماة.
4. مراجعة العزل الشبكي وضوابط الوصول ذي الامتيازات حول البنية التحتية الحرجة وبيئات البحث.
5. تأكيد مسارات تصعيد الحوادث، بما فيها الإبلاغ للهيئة الوطنية للأمن السيبراني عند الاقتضاء.