مجموعة يُشتبه بارتباطها بفيتنام تستهدف جهات في جنوب شرق آسيا ضمن حملة تجسس تتعلق ببحر الصين الجنوبي



كشفت SOCRadar عن حملة جديدة باسم WeaveLotus تُنسب إلى مجموعة مدعومة من فيتنام، تستهدف جهات عسكرية وحكومية وتشريعية في جنوب شرق آسيا لجمع معلومات عن شؤون الدفاع في بحر الصين الجنوبي.

- أطلقت SOCRadar اسم WeaveLotus على مجموعة النشاط غير الموثقة سابقاً.
- تُوصف المجموعة بأنها مدعومة من فيتنام، مع الإشارة إلى أن النسبة مشتبه بها.
- تستهدف الحملة جهات عسكرية وحكومية وتشريعية في جنوب شرق آسيا.
- الهدف المعلن هو جمع معلومات عن الاتفاقيات الدفاعية والعسكرية المتعلقة ببحر الصين الجنوبي.

- يُقدَّر أن النشاط شمل خمس عمليات اختراق في تايلاند.

نشرت SOCRadar تفاصيل مجموعة اختراقات لم تُوثَّق سابقاً، أطلقت عليها اسم WeaveLotus. وتُنسب الحملة إلى مجموعة قرصنة يُقدَّر أنها مدعومة من فيتنام، وهدفها التجسس وجمع المعلومات لا تحقيق مكاسب مالية.

ما ورد في التقرير

وفق التقرير، استهدفت المجموعة جهات عسكرية وحكومية وتشريعية في جنوب شرق آسيا، بغرض جمع معلومات عن الاتفاقيات الدفاعية والعسكرية المرتبطة ببحر الصين الجنوبي. ويُقدَّر أن النشاط تضمّن خمس عمليات اختراق في تايلاند.

ولا يتضمن المقتطف المتاح من المصدر تفاصيل تقنية مثل أساليب الاختراق أو الأدوات أو مؤشرات الاختراق، ولا يسمّي الجهات المتضررة، ولذلك لا نورد أي ادعاءات بشأنها.

الصلة بالمؤسسات في المملكة

لا يشير المصدر إلى أن جهات في المملكة كانت هدفاً لهذه الحملة. ومع ذلك فهي تذكير بأن عمليات التجسس المرتبطة بالدول تركّز عادةً على الجهات التي تحتفظ بمعلومات حساسة تتعلق بالسياسات والدفاع والعلاقات الدبلوماسية. وينبغي للجهات الحكومية وموّردي قطاع الدفاع والمؤسسات التي تتبادل المعلومات معهم أن تقيّم ما إذا كانت تحتفظ بمواد مماثلة.

والاستجابة المناسبة هي مراجعة الضوابط القائمة، لا ردّ فعل على تقرير واحد. وعند توفر النتائج التقنية الكاملة من SOCRadar، يمكن لفرق الأمن مقارنتها بما لديها من عمليات رصد.

ما يجب فعله الآن

1. الحصول على تقرير SOCRadar الكامل عن WeaveLotus ومطابقة أي مؤشرات منشورة مع سجلات الأنظمة وأدوات الكشف لديكم.
2. تحديد الأنظمة وصناديق البريد التي تحتوي معلومات دفاعية أو سياسية أو دبلوماسية والتأكد من مراقبتها وتقييد الوصول إليها.
3. مراجعة أمن تبادل المعلومات مع الشركاء والموّردين الذين يتعاملون مع مواد حكومية أو دفاعية حساسة.
4. توعية الإدارة التنفيذية والشؤون القانونية بهجمات التصيّد الموجّه ضد من يطّلعون على معلومات السياسات.
5. التأكد من أن عملية استخبارات التهديدات تغطي أنشطة التجسس المرتبطة بالدول وتغذّي الاستجابة للحوادث.