مجموعة مرتبطة بإيران تُدعى «Volant Manticore» تستهدف مؤسسات قبرصية بحسب تقرير



أفاد موقع Dark Reading بأن مجموعة إيرانية لم تُوثَّق سابقًا، تُعرف باسم Volant Manticore، تستهدف مؤسسات قبرصية ضمن جهد لجمع المعلومات الاستخباراتية لصالح طهران.

- تحمل المجموعة اسم Volant Manticore ولم يسبق توثيقها.
- توصف بأنها إيرانية وتعمل على جمع معلومات استخباراتية لصالح طهران.
- الأهداف المعلنة هي مؤسسات في قبرص.
- لا يتضمن المقتطف المتاح تفاصيل تقنية أو ضحايا أو مؤشرات اختراق.

ما الذي ورد في التقرير

أفاد موقع Dark Reading بأن مجموعة تهديد إيرانية لم تُوثَّق من قبل، تُعرف باسم "Volant Manticore"، تستهدف

مؤسسات في قبرص. ويوصف النشاط بأنه جزء من جهد لجمع المعلومات الاستخباراتية لصالح طهران، ما يشير إلى التجسس وليس التعطيل أو الكسب المالي.

المادة المتاحة لنا موجزة؛ فهي لا تسمّي الضحايا أو القطاعات أو أساليب الهجوم أو الأدوات أو مؤشرات الاختراق، ولن نذهب في التكهن إلى ما هو أبعد مما ذكره المصدر.

أهمية الخبر للمؤسسات السعودية

يتعلق التقرير بقبرص لا بالمملكة، ولم يرد فيه أي استهداف لجهات سعودية. ومع ذلك، فظهور مجموعة جديدة مرتبطة بدولة وتركّز على جمع المعلومات فرصة للمؤسسات الخاضعة للتنظيم في المنطقة للتأكد من قدرة منظومات الرصد واستخبارات التهديدات لديها على استيعاب أسماء الجهات المهاجمة الجديدة بسرعة. وتميل حملات التجسس إلى الهدوء والاستمرار طويلاً، لذا تعتمد الجاهزية على وضوح الرؤية لا على الاستجابة للتنبيهات وحدها.

الموقف الموصى به

لا حاجة لإجراءات طارئة استنادًا إلى هذا التقرير. والمناسب مراجعة هادئة: التأكد من أن مصادر استخبارات التهديدات ستوفّر مؤشرات خاصة بـ Volant Manticore عند نشرها، ومن أن الفرق تعرف كيف تتعامل معها. وتابعوا التقارير التقنية الأوسع من الباحثين الأصليين ومن الجهات الوطنية قبل تعديل الضوابط.

ما يجب فعله الآن

1. تأكدوا من أن مصادر استخبارات التهديدات لديكم ستوفّر مؤشرات Volant Manticore فور نشرها.
2. تحققوا من إمكانية إدخال أسماء الجهات المهاجمة ومؤشراتها الجديدة في SIEM وEDR بسرعة.
3. راجعوا الرصد الخاص بالاختراقات الهادئة طويلة الأمد على الأنظمة التي تحتوي معلومات حساسة.
4. تابعوا تنبيهات الهيئة الوطنية للأمن السيبراني والباحثين الأصليين للحصول على التفاصيل التقنية.
5. أبلغوا فريق الأمن بأنه لم يُبلَّغ عن استهداف سعودي، حتى تبقى الاستجابة متناسبة.