مجموعة Volant Manticore المرتبطة بإيران تستخدم باب KuboShell الخلفي عبر IPFS



وثّقت تقارير مجموعة تجسس جديدة مرتبطة بإيران باسم Volant Manticore استهدفت قطاعات الاتصالات والطيران والبنية التحتية الحرجة في قبرص، عبر باب خلفي يُسمى KuboShell يعتمد على IPFS للتحكم والسيطرة.

- Volant Manticore مجموعة تجسس إلكتروني جديدة لم تُوثَّق سابقًا ومرتبطة بإيران.
- شملت الأهداف المعلنة شركات اتصالات وشركات طيران وبنية تحتية حرجة في قبرص.
- يستخدم الباب الخلفي KuboShell نظام الملفات IPFS في التحكم والسيطرة.
- تنشر المجموعة إطار Homa لما بعد الاختراق، وهو إعادة تنفيذ لأداة قائمة.
- لا يتضمن المقتطف المتاح مؤشرات اختراق ولا ذكرًا لاستهداف جهات في المملكة.

وصف باحثون مجموعة تجسس إلكتروني جديدة لم تُوثَّق سابقًا تُدعى Volant Manticore، ويُرجَّح ارتباطها بإيران. وبحسب التقرير، استهدفت المجموعة شركات اتصالات وشركات طيران وبنية تحتية حرجة في قبرص.

ما هو معلوم

تتمحور عمليات المجموعة حول باب خلفي يُسمى **KuboShell**. وبدلاً من الاعتماد على خوادم تقليدية فقط، يستخدم نظام الملفات اللامركزي **IPFS** في التحكم والسيطرة. وبعد الوصول إلى البيئة، تنشر المجموعة إطار **Homa** لما بعد الاختراق، وهو إعادة تنفيذ لأداة قائمة.

ولا يذكر المقتطف المتاح مؤشرات اختراق ولا أسلوب الوصول الأولي ولا أي ضحايا في المملكة العربية السعودية.

أهمية الأمر للجهات في المملكة

القطاعات المذكورة، وهي الاتصالات والطيران والبنية التحتية الحرجة، من القطاعات الأساسية في المملكة أيضًا. وقد تبدو اتصالات التحكم عبر IPFS كحركة ويب اعتيادية، وقد تتجاوز الضوابط المعتمدة على سمعة النطاقات أو عناوين IP. لذا ينبغي للجهات في هذه القطاعات اعتبار التقرير فرصة لمراجعة تغطية الرصد، لا دليلاً على نشاط محلي.

النهج المقترح

انتظروا التقرير الفني الكامل والمؤشرات ثم طابقوها مع سجلاتكم. وفي الأثناء، تأكدوا من قدرتكم على رصد بوابات مشاركة الملفات اللامركزية والتحكم في الوصول إليها من الشبكات المؤسسية والتشغيلية.

ما يجب فعله الآن

1. الحصول على التقرير الفني الكامل ومطابقة أي مؤشرات منشورة مع سجلات الوكيل وDNS ونقاط النهاية.
2. مراجعة إمكانية الوصول إلى بوابات IPFS وعملائه من الشبكات المؤسسية والتشغيلية، وتقييدها عند غياب الحاجة التشغيلية.
3. إضافة قواعد رصد للاتصالات الصادرة غير المعتادة نحو خدمات التخزين اللامركزي من الخوادم والأنظمة الحساسة.
4. التحقق من تغطية أنظمة الاتصالات والطيران والبنية التحتية الحرجة بحلول EDR وبالتسجيل المركزي للسجلات.
5. مشاركة النتائج ذات الصلة مع الهيئة الوطنية للأمن السيبراني ونظراء القطاع عبر القنوات المعتمدة.