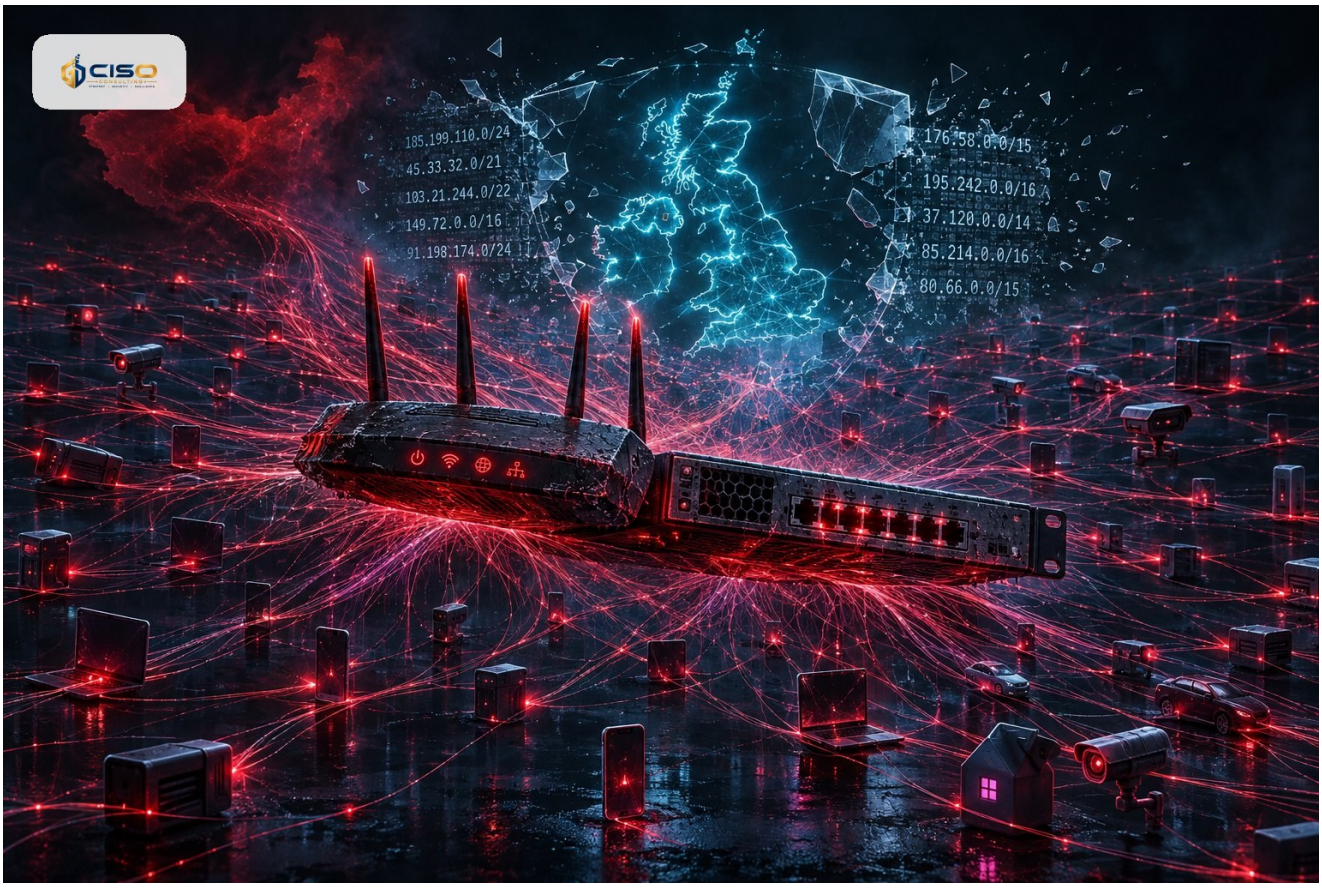
المركز الوطني للأمن السيبراني في بريطانيا: جهات صينية الصلة تستخدم شبكات خفية من الأجهزة الطرفية المخترقة



يحذّر المركز الوطني للأمن السيبراني البريطاني وشركاؤه من استخدام جهات صينية الصلة شبكات بوت نت من أجهزة توجيه وأجهزة طرفية مخترقة، ما يُضعف قوائم الحظر الثابتة. ويقدّم الإرشاد خطوات للرصد والتأسيس وانعدام الثقة.

- انتقلت الجهات الصينية الصلة من بنية تحتية تُشترى بشكل منفرد إلى شبكات خفية واسعة تُبنى من أجهزة توجيه وأجهزة طرفية مخترقة.
- تخدم هذه الشبكات كل مراحل سلسلة الهجوم، من الاستطلاع إلى تسريب البيانات.
- تُجدَّد العقد باستمرار وتُشارَك بين مجموعات تهديد عدة، فتختفي مؤشرات الاختراق بسرعة اكتشافها.
- المؤسسات التي تعتمد على دفاعات ثابتة فقط معرّضة للتجاوز.

- يتضمن الإرشاد توجيهات منفصلة للمنظمات الصغيرة والمتوسطة والكبيرة.

نشر المركز الوطني للأمن السيبراني البريطاني (NCSC)، بالتعاون مع Cyber League والجهات المشاركة في الاعتماد، إرشاداً حول تحوّل في طريقة بناء الجهات الصينية الصلة لبنيتها التحتية الهجومية. فبدل شراء خوادم بصورة منفردة، تشغّل هذه الجهات بشكل متزايد شبكات خفية واسعة، هي شبكات بوت نت مكوّنة من أجهزة توجيه وأجهزة طرفية مخترقة.

ملامح التهديد

تُستخدم هذه الشبكات في كل مراحل الاختراق، ومنها الاستطلاع وتسليم البرمجيات الخبيثة والقيادة والتحكم وتسريب البيانات. ويصفها المركز بأنها منخفضة التكلفة وقابلة للإنكار وسريعة إعادة التشكيل، ما يجعل قوائم حظر عناوين IP الثابتة غير فعّالة.

ولأن الشبكات تُجدَّد باستمرار وتتشارك عقدها مجموعات تهديد متعددة، يواجه المدافعون ما يسميه المركز «انقراض مؤشرات الاختراق»، إذ تختفي المؤشرات بالسرعة نفسها التي تُكتشف بها. ويتمثل الأثر في سرقة بيانات حساسة واحتمال تعطيل خدمات حيوية.

ما يوصي به الإرشاد

يقدّم الإرشاد توجيهات للمنظمات الصغيرة والمتوسطة والكبيرة. وعلى جميع المنظمات:

- رسم خريطة لحركة الأجهزة الطرفية وتحديد خط أساس لها، خصوصاً اتصالات VPN والوصول عن بُعد.
- اعتماد تصفية ديناميكية عبر مصادر معلومات التهديد تشمل مؤشرات الشبكات الخفية المعروفة.

وعلى المنظمات المعرّضة للاستهداف إضافة المصادقة الثنائية للوصول عن بُعد، وتطبيق ضوابط انعدام الثقة وقوائم السماح بعناوين IP والتحقق من شهادات الأجهزة حيثما أمكن. أما الجهات الكبيرة أو عالية المخاطر فعليها النظر في الصيد الاستباقي لحركة أجهزة SOHO وإنترنت الأشياء المشبوهة، والتحليل الجغرافي، وكشف الشذوذ بالتعلم الآلي.

ويخلص المركز إلى أن التطبيق السريع لإجراءات الرسم وخط الأساس وانعدام الثقة ضروري لتقليل التعرض. ولا يتطرق المصدر إلى استهداف خاص بالمملكة.

ما يجب فعله الآن

1. حصر الأجهزة الطرفية (أجهزة التوجيه وبوابات VPN والوصول عن بُعد) وتحديد خط أساس لحركتها الطبيعية.
2. فرض المصادقة متعددة العوامل على جميع خدمات الوصول عن بُعد وVPN.
3. عدم الاكتفاء بقوائم حظر IP الثابتة، واعتماد تصفية ديناميكية عبر مصادر تهديد محدّثة باستمرار.
4. تطبيق قوائم السماح بعناوين IP والتحقق من شهادات الأجهزة وانعدام الثقة على الاتصالات عن بُعد حيثما أمكن.
5. للجهات الكبيرة أو عالية المخاطر: تقييم الصيد الاستباقي لحركة SOHO وإنترنت الأشياء وكشف الشذوذ

في حركة الأجهزة الطرفية.

6. مراجعة الإرشاد الكامل للمركز البريطاني ومواءمته مع ضوابط الهيئة الوطنية للأمن السيبراني (ECC) وإطار الأمن السيبراني للبنك المركزي السعودي.