

## وكالات سبيرانية دولية تصدر إرشادات مشتركة للتصدي للشبكات الخفية المرتبطة بالصين



نشر المركز الوطني للأمن السبيرانى البريطانى و15 شريكاً دولياً إرشادات حول الشبكات الخفية من الأجهزة المخترقة التي تستخدمها جهات مرتبطة بالصين لإخفاء هجماتها، مع تحذير من «انقراض مؤشرات الاختراق».

- تُبنى الشبكات الخفية غالباً من أجهزة طرفية مخترقة مثل الراوترات المنزلية والأجهزة الذكية، وتُستخدم لإخفاء مصدر الهجمات.
- تفيد الإرشادات بأن معظم الجهات المرتبطة بالصين يُعتقد أنها تعتمد هذه الأساليب، وأن الشبكات تُستخدم على نطاق واسع ضد القطاعات الحيوية لسرقة البيانات والحفاظ على وصول مستمر.
- تحذّر من «انقراض مؤشرات الاختراق»، إذ تختفي المؤشرات بسرعة اكتشافها، ما يستلزم إجراءات تكيفية قائمة على المعلومات الاستخبارية.

- تذكر أن هذه الشبكات تُنشأ وتُدار من خارج الجهات المهاجمة على يد شركات صينية لأمن المعلومات.
- من التوصيات رسم خط أساس لحركة الأجهزة الطرفية، وخاصة VPN والوصول عن بُعد، واعتماد تصفية ديناميكية لمصادر التهديد.

نشر المركز الوطني للأمن السيبراني البريطاني (NCSC)، التابع لهيئة GCHQ، إرشادات مشتركة مع جهات من القطاع الصناعي و15 شريكاً دولياً حول سبل التصدي للشبكات الخفية. وصدرت في اليوم الثاني من مؤتمر CYBERUK 2026.

## ما الذي تقوله الإرشادات

تتألف الشبكات الخفية عادةً من أجهزة طرفية يومية متصلة بالإنترنت وسهلة الاختراق، مثل الراوترات المنزلية والأجهزة الذكية، بعد السيطرة عليها. ويستخدمها المهاجمون لإخفاء المصدر الحقيقي للعمليات وتفاخي نسبها إليهم. وبحسب الإرشادات تُستخدم هذه الشبكات على نطاق واسع لاستهداف القطاعات الحيوية حول العالم وسرقة البيانات الحساسة والحفاظ على وصول مستمر.

وتصف الجهات المُعدّة تحولاً متعمداً لدى مجموعات مقرها الصين نحو هذه الشبكات، وتذكر أنها تُنشأ وتُدار من خارج تلك المجموعات على يد شركات صينية لأمن المعلومات. وتشير المصدر إلى أن المركز وشركاءه سقّوا في سبتمبر 2024 شركة Integrity Technology Group بوصفها المتحكمة في شبكة botnet استخدمتها مجموعة Flax Typhoon، وأن الحكومة البريطانية فرضت عليها عقوبات في ديسمبر 2025.

## أهمية ذلك للمدافعين

تبرز الإرشادات مشكلة «انقراض مؤشرات الاختراق» (IOC extinction)، أي اختفاء المؤشرات بالسرعة نفسها التي تُكتشف بها، ما يُضعف قيمة قوائم الحظر الثابتة، ويستدعي إجراءات أكثر تكيفاً تستند إلى المعلومات الاستخباراتية. ويوصي الملخص التنفيذي بأن ترسم المنظمات خط أساس لحركة الأجهزة الطرفية، وخاصة اتصالات VPN والوصول عن بُعد، وأن تعتمد تصفية ديناميكية لمصادر التهديد تشمل مؤشرات الشبكات الخفية المعروفة.

وللمرونة الأوسع، يوجّه المركز المنظمات الصغيرة إلى أداة Cyber Action Toolkit المجانية، والكبيرة إلى شهادة Cyber Essentials وإطار Cyber Assessment Framework المحدّث.

وشاركت في اعتماد الإرشادات جهات من أستراليا وكندا وألمانيا واليابان وهولندا ونيوزيلندا وإسبانيا والسويد والولايات المتحدة.

## ما يجب فعله الآن

1. حصر الأجهزة الطرفية (الراوترات وبوابات VPN وأجهزة الوصول عن بُعد) ووضع خط أساس لحركتها الاعتيادية لتسهيل رصد الانحرافات.
2. مراجعة سجلات VPN والوصول عن بُعد بحثاً عن اتصالات من عناوين سكنية أو استهلاكية لا تتوافق مع سلوك المستخدمين المتوقع.
3. الانتقال من قوائم الحظر الثابتة لمؤشرات الاختراق إلى تصفية ديناميكية لمصادر التهديد تشمل

مؤشرات الشبكات الخفية.

4. تحديث الأجهزة الطرفية وتحسينها وإيقاف غير المدعوم منها، وإزالة أي تعرّض غير ضروري لواجهات الإدارة على الإنترنت.

5. قراءة الإرشادات والملخص التنفيذي الكاملين على موقع NCSC وربط إجراءات المعالجة بضوابط NCA وSAMA CSF وECC.

6. الاستفسار من مزودي الخدمات المُدارة والمعلومات الاستخبارية عن آلية تعاملهم مع المؤشرات سريعة التغير.