

شبكات الأجهزة المخترقة الخفية: إرشادات مشتركة للدفاع ضد الجهات المرتبطة بالصين



أفادت NCSC-UK وجهات شريكة أن الجهات المرتبطة بالصين باتت توجّه نشاطها عبر شبكات واسعة من الأجهزة المخترقة، أغلبها راوترات SOHO وأجهزة IoT. وتقل فاعلية قوائم الحظر الثابتة، وتعرض الإرشادات دفاعات متعددة الطبقات.

- انتقلت الجهات المرتبطة بالصين من البنية التحتية المشتراة بشكل فردي إلى شبكات كبيرة من الأجهزة المخترقة تُوفّر خارجياً.
- تتكون هذه الشبكات غالباً من راوترات SOHO، إضافة إلى أجهزة IoT وجدران حماية وأجهزة NAS، وكانت أجهزة الحافة المنتهية الدعم نقطة ضعف رئيسية.
- تُستخدم في كل مراحل الهجوم من الاستطلاع حتى تسريب البيانات، وقد تخدم الشبكة الواحدة عدة جهات.
- لأن العقد تتغير باستمرار، تقل فاعلية قوائم حظر عناوين IP الخبيثة الثابتة.

- تتدرج التوصيات بحسب حجم المنظمة ومستوى المخاطر، من حصر أجهزة الحافة والمصادقة متعددة العوامل إلى الصيد الاستباقي.

ما الذي تغيّر

تفيد NCSC-UK، بالتعاون مع جهات من أستراليا وكندا وألمانيا واليابان وهولندا ونيوزيلندا وإسبانيا والسويد والولايات المتحدة، بتحول كبير في أسلوب عمل الجهات المرتبطة بالصين. فبدل شراء بنية تحتية خاصة بها، تعتمد غالبيتها الآن على شبكات واسعة من الأجهزة المخترقة تسميها الإرشادات «الشبكات الخفية». وتتكون أساساً من راوترات المكاتب الصغيرة والمنازل (SOHO) إضافة إلى أجهزة IoT والأجهزة الذكية.

وتذكر الإرشادات مجموعة Volt Typhoon التي استخدمت شبكات كهذه لتثبيت قدرات مسبقة في بنى تحتية وطنية حرجية، ومجموعة Flax Typhoon التي استخدمت شبكة أخرى للتجسس. كما تشير إلى Raptor Train التي أصابت أكثر من 200,000 جهاز في 2024، وإلى KV Botnet المبنية في معظمها على راوترات NetGear Cisco الضعيفة والمنتھية الدعم.

أهمية ذلك للمدافعين

تدخل حركة المرور عادة عبر عقدة دخول، ثم تمر بعدة عقد وسيطة مخترقة، وتخرج من عقدة خروج غالباً في المنطقة الجغرافية للهدف. لذلك قد يبدو الهجوم قادماً من أجهزة محلية عادية. ولأن الشبكات تتغير باستمرار وقد تخدم عدة جهات، تقل فاعلية قوائم حظر IP الثابتة.

ما توصي به الإرشادات

على جميع المنظمات حصر أجهزة الحافة، وتحديد خط أساس للاتصالات الطبيعية بالشبكات الخاصة الافتراضية، واستخدام مصادر تهديد ديناميكية تغطي الشبكات الخفية، وفرض المصادقة متعددة العوامل للوصول عن بُعد. وعلى المنظمات الأعلى خطراً النظر في قوائم السماح ونهج الثقة المعدومة وشهادات الأجهزة وتقليل الحضور المكشوف على الإنترنت. أما الأكثر عرضة فعلية الصيد الاستباقي وتتبع الشبكات الخفية كجهات تهديد مستقلة. وتنبّه الإرشادات إلى أن هذه الخطوات لا تزيل كل المخاطر.

ما يجب فعله الآن

1. حصر جميع أجهزة حافة الشبكة (الراوترات وجدران الحماية وNAS والكاميرات) وإيقاف أو استبدال الأجهزة المنتھية الدعم.
2. تحديد خط أساس لمصادر الوصول المشروعة عبر VPN والوصول عن بُعد، ومراجعة الاتصالات القادمة من نطاقات الإنترنت المنزلي.
3. فرض المصادقة متعددة العوامل على كل وصول عن بُعد.
4. الاشتراك في مصادر تهديد ديناميكية تشمل بنية الشبكات الخفية، وعدم الاكتفاء بقوائم الحظر الثابتة.
5. للأنظمة عالية الخطورة: تطبيق قوائم السماح ونهج الثقة المعدومة وشهادات الأجهزة للاتصالات VPN، وتقليل الخدمات المكشوفة على الإنترنت.
6. عند توفر القدرة، الصيد عن اتصالات صادرة من نطاقات راوترات SOHO أو أجهزة IoT وتتبع الشبكات

الخفية المعلن عنها.