

المركز الوطني للأمن السيبراني البريطاني: APT28 يخترق أجهزة التوجيه الضعيفة لإعادة توجيه حركة الإنترنت وسرقة بيانات الدخول



يفيد تحذير المركز الوطني للأمن السيبراني البريطاني بأن مجموعة APT28 الروسية استغلت أجهزة توجيه ضعيفة لتنفيذ اختطاف DNS واعتراض الحركة وسرقة كلمات المرور ورموز الوصول، ويدعو إلى تأمين واجهات الإدارة والتحديث والتحقق بخطوتين.

- استغلت APT28 أجهزة توجيه ضعيفة لتنفيذ اختطاف DNS وإعادة توجيه حركة المستخدمين عبر خوادم يتحكم بها المهاجمون.
- كان الهدف اعتراض الحركة وجمع كلمات المرور ورموز الوصول من خدمات الويب والبريد الإلكتروني الشخصية.
- يُرجَّح أن النشاط انتهازي، إذ يشمل ضحايا كثيرًا ثم يضيّق نطاقه إلى أهداف ذات قيمة استخباراتية.
- سبق أن ربطت المملكة المتحدة APT28 بالاستخبارات العسكرية الروسية (GRU) والوحدة

- تشمل التوصيات حماية واجهات الإدارة وتحديث الأجهزة والبرمجيات وتفعيل التحقق بخطوتين.

نشر المركز الوطني للأمن السيبراني في المملكة المتحدة، وهو جزء من GCHQ، تحذيرًا يوضح كيف اخترقت مجموعة APT28 المرتبطة بالدولة الروسية أجهزة توجيه واسعة الاستخدام، ما أتاح لها إعادة توجيه حركة الإنترنت الخاصة بالمستخدمين خفية عبر خوادم خبيثة تتحكم بها.

ما يصفه التحذير

استخدم المهاجمون أجهزة توجيه ضعيفة لدعم عمليات اختطاف DNS. وخدمة DNS هي التي تتيح الوصول إلى المواقع بأسمائها المألوفة بدل عناوين IP. وعند العبث بها يمكن توجيه المستخدمين إلى مواقع خبيثة مصممة لسرقة بيانات الدخول. ووفق التحذير، أتاح ذلك اعتراض الحركة وجمع بيانات الاعتماد، ومنها كلمات المرور ورموز الوصول، من خدمات الويب والبريد الإلكتروني الشخصية.

ويرجح المركز أن النشاط انتحاري، إذ تستهدف المجموعة أعداءًا كبيرة من الضحايا المحتملين أولاً، ثم تركز على من يمثل قيمة استخباراتية مع تطور العملية. وقد سبق أن نسبت المملكة المتحدة APT28 إلى مركز الخدمات الخاصة الرئيسي رقم 85 في الاستخبارات العسكرية الروسية (GRU)، الوحدة العسكرية 26165. وتُعرف المجموعة أيضًا بأسماء Sofacy و Sednit Gang و Forest Blizzard و Fancy Bear.

الأهمية للجهات المنظمة

يذكر التحذير بأن أجهزة الحافة، مثل أجهزة التوجيه، قد تكون منفذًا لسرقة بيانات الدخول، بما في ذلك من الموظفين الذين يعتمدون على شبكات منزلية أو مكاتب صغيرة. ولا يشير المصدر إلى نشاط في المملكة العربية السعودية، لكن الأساليب المذكورة تنطبق على أي جهة تعتمد أجهزة مشابهة.

وتتركز توصيات المركز على حماية واجهات إدارة الأنظمة، وإبقاء الأجهزة والبرمجيات مصانة ومحدّثة، وتفعيل التحقق بخطوتين. ويُشجّع المدافعون عن الشبكات على الاطلاع على التحذير كاملاً وتطبيق إرشاداته.

ما يجب فعله الآن

1. حصر أجهزة التوجيه وأجهزة الحافة الأخرى المستخدمة، بما فيها أجهزة الفروع والفروع والعمل عن بُعد، والتأكد من تحديث برامجهما الثابتة.
2. تقييد واجهات الإدارة بحيث لا تكون متاحة عبر الإنترنت ولا يُوصل إليها إلا من شبكات إدارية موثوقة.
3. مراجعة إعدادات DNS على أجهزة الحافة بحثًا عن خوادم تحليل غير متوقعة أو تغييرات، ومراقبة أي انحراف في الإعدادات.
4. فرض التحقق بخطوتين على البريد الإلكتروني وخدمات الويب والوصول عن بُعد حتى لا تكفي كلمة المرور المسروقة وحدها.
5. إطلاع فريق الأمن على الأساليب الواردة في تحذير NCSC وإدراج اختطاف DNS ضمن سيناريوهات الكشف والاستجابة للحوادث.