

مجموعة APT28 تخترق أجهزة التوجيه الضعيفة وتتلاعب بإعدادات DNS لسرقة بيانات الاعتماد



أفاد المركز الوطني للأمن السيبراني في المملكة المتحدة بأن APT28 استغلت أجهزة توجيه ضعيفة لتغيير إعدادات DHCP/DNS وتنفيذ هجمات وسيط تسرق كلمات المرور ورموز OAuth.

- غيّرت APT28 إعدادات DHCP/DNS في أجهزة توجيه مخترقة لتتم معالجة الطلبات عبر خوادم DNS يملكها المهاجم.
- هدفت هجمات الوسيط الناتجة إلى سرقة كلمات المرور ورموز OAuth لخدمات الويب والبريد.
- من الأجهزة المستغلة TP-Link WR841N على الأرجح عبر CVE-2023-50224، واستُهدفت طرازات TP-Link أخرى كثيرة.
- يبدو أن النشاط، الممتد من 2024 إلى 2026، انتهازي ثم تُصَفَّى الضحايا بحسب قيمتهم الاستخبارية.
- شملت النطاقات المستهدفة عدة نطاقات مرتبطة بـ Outlook، وينصح المركز باعتماد كشف

نشر المركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC) تفاصيل عن كيفية استغلال الجهة الروسية APT28 لأجهزة التوجيه في اختطاف DNS. ويقيم المركز أن المجموعة هي على الأرجح بدرجة شبه مؤكدة الوحدة 26165 التابعة للاستخبارات العسكرية الروسية (GRU).

ما الذي تفعله الجهة المهاجمة

تستغل APT28 ثغرات في أجهزة توجيه، وأغلبها أجهزة المكاتب الصغيرة والمنازل، وتعيد كتابة إعدادات DNS ضمن DHCP لتشير إلى خوادم يملكها المهاجم. وترث الأجهزة المتصلة، كالحواسيب المحمولة والهواتف، هذه الإعدادات. فتُحلّ النطاقات المرتبطة بالبريد أو صفحات تسجيل الدخول إلى بنية تحتية للمهاجم، بينما تُحلّ بقية الطلبات إلى عناوينها الشرعية، مما يساعد على إخفاء النشاط.

ثم تحاول المجموعة تنفيذ هجمات الوسيط (AitM) على الاتصالات اللاحقة، في المتصفحات وتطبيقات سطح المكتب، لالتقاط كلمات المرور ورموز OAuth أو ما يشبهها. ويرجح المركز أن الحملة انتهازية: تُرصد شريحة واسعة من المستخدمين أولاً ثم تُصقّى بحثاً عن ضحايا ذوي قيمة استخباراتية محتملة.

من الأجهزة المستغلة TP-Link WR841N على الأرجح عبر CVE-2023-50224، وهي ثغرة تتيح لمهاجم غير مصادق الحصول على بيانات الاعتماد عبر طلبات HTTP GET مصممة خصيصاً. ثم يغيّر طلب ثانٍ إعدادات DNS. ويورد التقرير طرازات TP-Link أخرى كثيرة، كما شملت مجموعة بنية ثانية أجهزة TP-Link و MikroTik.

أهمية الأمر

قد تعيد أجهزة التوجيه في الفروع ومنازل الموظفين عن بُعد والمواقع الصغيرة توجيه حركة المصادقة بصمت، فتتكشف بيانات اعتماد البريد والخدمات. وينبه المركز إلى أن المؤشرات المحددة قابلة للتغير، لذا ينبغي الاعتماد على أساليب كشف أشمل لا على قوائم عناوين IP وحدها.

ومن توصيات المركز عدم تعريض واجهات الإدارة للإنترنت أبداً، وإبقاء الأجهزة والشبكات محدثة بتطبيق التحديثات الأمنية سريعاً، واستخدام أنظمة وبرمجيات حديثة.

ما يجب فعله الآن

1. حصر أجهزة التوجيه في الفروع ومواقع العمل عن بُعد والمكاتب الصغيرة، وتحديد طرازات TP-Link و MikroTik ومنها المدرجة في تقرير المركز.
2. التحقق من إعدادات DHCP/DNS في هذه الأجهزة مقارنةً بالمحللات المعتمدة، والتحقق في أي عناوين خوادم DNS غير معروفة.
3. التأكد من عدم إتاحة واجهات إدارة أجهزة التوجيه من الإنترنت، وتطبيق أحدث التحديثات الأمنية من المصنّع ومنها ما يعالج CVE-2023-50224.
4. مراقبة سجلات DNS وتسجيل الدخول لرصد أي تحليل غير معتاد لنطاقات البريد وتسجيل الدخول، أو عمليات دخول من بنية غير متوقعة.
5. مراجعة رموز OAuth والجلسات للحسابات المحتمل تعرضها، وإعادة تعيين بيانات الاعتماد عند اكتشافها.

