برمجيات الوكيل السكني على شبكة البيت الأبيض: دعوة لمراجعة شبكتك



رصد باحثون برمجيات وكيل سكني على أجهزة موظفين في البيت الأبيض جعلت عناوين IP متاحة للتأجير العام. وتنتشر هذه البرمجيات في شبكات الشركات والجهات الحكومية، ما يستدعي فحصًا داخليًا.

- رصدت Layer3 Intel عقد وكيل سكني تتصل من شبكة المكتب التنفيذي للرئيس (AS2650) بين 5 أكتوبر و3 نوفمبر.
- خرجت الحركة من الشبكة 236 مرة عبر ستة عناوين في 26 يومًا من 30، وغالبها بين الخامسة مساءً ومنتصف الليل.
- ربطت Synthient جزءًا من النشاط بتثبيتات Windows 11 لبرنامج Infatica، وهو برنامج وكيل يُدمج غالبًا في التطبيقات المجانية.
- وجدت Layer3 أن 28 خدمة وكيل منفصلة قادرة على الخروج عبر هذه الشبكة، ويمكن لأي

شخص استخدامها مقابل بضعة دولارات.

- تشير بيانات Spur وInfoblox إلى انتشار هذه الوكلاء في شبكات حكومية ومرافق وقطاعات صحية ومالية.

أفاد باحثون في الأمن السيبراني بأن عددًا من موظفي البيت الأبيض يستخدمون حواسيب أو أجهزة محمولة تعمل عليها برمجيات وكيل سكني، تتيح لأطراف خارجية استئجار عنوان الإنترنت الخاص بالجهاز. ولم يرد البيت الأبيض على طلب التعليق وقت النشر.

ما الذي رُصد

رصدت Layer3 Intel عقد وكيل تتصل بصورة متكررة من الشبكة المخصصة للمكتب التنفيذي للرئيس (AS2650) بين 5 أكتوبر و3 نوفمبر. وخرجت الحركة 236 مرة عبر ستة عناوين في 26 يومًا من أصل 30، وغالبها في المساء. وربطت Synthient جزءًا من النشاط بتثبيتات Windows 11 لبرنامج Infatica، وهو برنامج وكيل يُدمج كثيرًا في التطبيقات المجانية للحاسب والجوال. وذكرت Layer3 أن 28 خدمة وكيل منفصلة استطاعت الخروج عبر الشبكة، وأنها اكتشفت ذلك مصادفة دون استهداف الشبكة.

لماذا يهم ذلك

تتيح الوكلاء السكنية للعملاء إخفاء مصدرهم، فتبدو الحركة قادمة من عنوان المضيف. وترتبط هذه الخدمات بالاستيلاء على الحسابات والاحتيال الإعلاني وجمع المحتوى آليًا. كما أتاحت ثغرات فيها للمجرمين الوصول إلى أجهزة في الشبكات المحلية للمضيفين، واضطر عشرات المزودين إلى الترقيع في يناير 2026. وأشار أحد مؤسسي Synthient إلى أن بعض الموزعين يتيحون الشراء دون التحقق من هوية العميل.

ولا تقتصر المشكلة على الجهات الحكومية؛ إذ رصدت Spur وكلاء سكنية في نحو 300 شبكة حكومية و318 شركة مرافق و166 جهة صحية و141 شركة مصرفية ومالية، ووجدت Infoblox أن 65% من عملائها يستعلمون عن نطاقات مرتبطة بها. وغالبًا يعود السبب إلى تطبيق يضم حزمة تطوير تدفع للمطور عن كل تثبيت، على جهاز أحضره موظف إلى العمل.

على الجهات المنظمة اعتبار ذلك فرصة لفحص بيئتها عمليًا، لا سببًا للقلق.

ما يجب فعله الآن

1. استعلموا في سجلات DNS والوكيل عن النطاقات وأنماط الحركة المرتبطة بخدمات الوكيل السكني، ومنها Infatica.
2. احصوا التطبيقات على أجهزة المنشأة والأجهزة الشخصية المستخدمة في العمل، وأزيلوا البرامج المجانية التي تضم حزم وكيل.
3. طبقوا قوائم السماح بالتطبيقات وقيّدوا صلاحيات التثبيت على الأجهزة الطرفية.
4. فعّلوا التنبيه على الاتصالات الصادرة من نطاقات عناوينكم العامة إلى شبكات وكيل معروفة، خاصة في ساعات المساء.
5. أدرجوا حزم الوكيل السكني في سياسات الأجهزة الشخصية والاستخدام المقبول، وأطلعوا الموظفين

عليها.

6. افصلوا حركة الضيوف والأجهزة الشخصية عن الأنظمة الداخلية.