تطبيق عبر Microsoft Store يُستخدم لنشر Vinci RAT من خلال موقع مزيّف لأداة القصاصات



وصفت eSentire هجومًا استُخدم فيه تطبيق عبر Microsoft Store لنشر Vinci RAT، وهو trojan للتحكم عن بُعد. يُحوَّل الضحايا إلى موقع مزيّف لأداة قصاصات يقدّم مثبّتًا موقّعًا من Microsoft.

- كشف باحثون عن هجوم استخدم تطبيقًا عبر Microsoft Store لنشر Vinci RAT.
- Vinci RAT هو remote access trojan يتيح التحكم في النظام عن بُعد.
- وفق eSentire تبدأ السلسلة بإعادة توجيه إلى موقع مزيّف لأداة القصاصات.
- يقدّم الموقع مثبّتًا موقّعًا من Microsoft باسم Snipping-Tool.exe.
- لا يذكر المقتطف المتاح أعداد الضحايا أو تفاصيل تقنية إضافية.

نشر باحثون في الأمن السيبراني تفاصيل هجوم استخدم فيه المهاجم تطبيقًا عبر Microsoft Store لنشر remote

access trojan يُعرف باسم Vinci RAT، وتنسب النتائج إلى eSentire.

ما الذي أُعلن

وفق eSentire يبدأ الهجوم عندما يُحوَّل المستخدم إلى موقع مزيّف يتظاهر بأنه مصدر لأداة قصاصات الشاشة. ومن هذا الموقع يُقدَّم مثبّت موقّع من Microsoft باسم "Snipping-Tool.exe". ويمكن لهذا الـ trojan أن يمنح المشغّل تحكمًا عن بُعد في الجهاز المصاب.

النص المتاح من المصدر مقتطف، ولذلك لا يصف مراحل العدوى اللاحقة ولا حجم الحملة ولا الجهات الفاعلة. ولم نضف شيئًا يتجاوز ما ورد.

لماذا يهم ذلك

قد يجعل التوقيع الرقمي من Microsoft أو الارتباط بـ Microsoft Store المثبّت يبدو موثوقًا للمستخدمين ولبعض الضوابط. وعلى المؤسسات التي تعدّ التوقيع أو مصدر المتجر دليلاً على السلامة أن تدرك أن هذه الإشارة وحدها لم تكن كافية هنا.

الخطوات المقترحة

تعامل مع الأدوات المساندة مثل أدوات التقاط الشاشة كبرمجيات تحتاج إلى اعتماد، حتى لو بدت قادمة من متجر موثوق. وتحقق من ظهور المثبّت أو النطاق المذكور في بيئتك، وذكّر الموظفين بتثبيت الأدوات عبر القنوات المعتمدة فقط.

ما يجب فعله الآن

1. ابحث في سجلات نقاط النهاية والـ proxy عن النطاق snipp.codes-team[.]com وعن الملف Snipping-Tool.exe.
2. احظر النطاق المذكور على بوابة الويب وطبقة DNS.
3. قيّد Microsoft Store وتثبيت البرامج من المستخدمين بقائمة تطبيقات معتمدة.
4. لا تعتمد على توقيع Microsoft وحده دليلاً على السلامة، وطبّق القوائم المسموحة وفحوص السمعة.
5. ذكّر الموظفين بالحصول على الأدوات من القنوات الداخلية المعتمدة فقط والإبلاغ عن أي إعادة توجيه غير متوقعة.
6. عند العثور على المثبّت اعزل الجهاز وابدأ إجراءات الاستجابة للحوادث.