الخليج

اقتصاد, تقنية وسيارات

6 نوفمبر 2023 16:17 مساء

تهديدات خبيثة تستهدف الخدمات المصرفية.. لسرقة البيانات والأموال 3

«دبي: «الخليج

كشف أحدث تقرير عن برمجيات الجريمة لكاسبرسكي عن ثلاثة تهديدات خبيثة قادرة على سرقة البيانات والأموال وقام بتحليلها، وهي: أداة سرقة البيانات «جو بيكس»، التي تستهدف نظام الدفع البرازيلي «بيكس»، بالإضافة إلى أداة سرقة البيانات متعددة الوظائف «لومار»، وسلالة برمجيات الفدية «آر هايسيدا»، ومع استمرار نمو التهديدات السيبرانية ذات الدوافع المالية، يحث خبراء كاسبرسكي المستخدمين على توخي الحذر الدائم.

وكان أول تهديد تناوله التقرير، وهو حملة خبيثة تعمل منذ ديسمبر 2022، وتركز على استهداف نظام الدفع «بيكس» المستخدم على نطاق واسع في البرازيل.

تبدأ استراتيجية «جو بيكس»، عندما يبحث المستخدمون عن نسخة الويب من تطبيق واتساب في محرك البحث، إذ تستخدم الحملة إعلانات خادعة لاستدراج الضحايا، حيث تستخدم الحملة أداة مكافحة الاحتيال من منصة «آي بي

كواليتي سكور»، لتمييز المستخدمين الحقيقيين عن الروبوتات، وتقدم خياري تحميل استناداً إلى حالة المنفذ 27275 المرتبط ببرنامج حماية الخدمات المصرفية، وصُممت هذه البرمجية الخبيثة لسرقة بيانات المعاملات المصرفية والتلاعب بها، وهي مرنة في تنفيذ مراحل مختلفة والاستجابة للأوامر الصادرة عن خادم القيادة والتحكم (C2).

• إمكانات هائلة

أما أداة سرقة البيانات متعددة الوظائف، فقد استعرضها مستخدم يُدعى «كوليكتور»، لأول مرة في يوليو 2023. وتتمتع الأداة بإمكانات هائلة منها تسجيل جلسات المستخدمين على تطبيق تلجرام، وجمع كلمات المرور، وملفات تعريف، وبيانات الملء التلقائي، مع استرداد الملفات من آلات الحاسوب للمستخدمين، واستخراج البيانات من مختلف محافظ العملات المشفرة. بالمقابل، تتميز أداة «لومار» بحجمها الصغير الناتج عن برمجتها بلغة «سي»، ولو أن هذا الحجم الصغير لا يحد من قدراتها. فبمجرد تشغيلها، تقوم الأداة بجمع معلومات النظام وبيانات المستخدم، ثم ترسلها إلى خادم قيادة وتحكم (C2). يستضيف مطور وتستفيد عملية جمع البيانات هذه من استخدام ثلاثة خيوط معالجة منفصلة. الأداة خادم قيادة وتحكم خاصاً به ويعامله كمزود برمجيات خبيثة مثل خدمة «إم أي أي إس»، ويوفر هذا الخادم ميزات تسهل الاستخدام مثل التحليلات وسجلات البيانات. ويمكن للمستخدمين تحميل أحدث إصدار من الأداة، وتلقي إشعارات على تلجرام عن البيانات الواردة.

دخلت برمجية الفدية «آر هايسيدا» حديثاً على ساحة برمجيات الفدية كخدمة «آر أي أي إس»، إذ اكتشفتها قراءات كاسبرسكي في شهر مايو/ أيار. وتتميز هذه البرمجية باستخدامها آلية حذف ذاتي فريدة، كما أنها تتوافق مع إصدارات أنظمة التشغيل السابقة لنظام ويندوز 10.

يذكر أن تصميم الأداة معقد للغاية؛ فكود البرمجية مكتوب بلغة «سي + +»، وتم تجميعها باستخدام أداة «مين جي دبليو»ومكتبات مشتركة. وعلى الرغم من حداثة هذه الأداة النسبية، إلا أن البرمجية قد واجهت تحديات إعداد أولية مع خادم الموجه البصلي الخاص بها، ما كشف عن قدرة المجموعة المطورة لها على التكيُّف والتعلّم السريع.

• دوافع مالية

وقال يورنت فاندر ويل، باحث أمن متقدم في فريق البحث والتحليل العالمي لدى كاسبرسكي: «مع تزايد التهديدات السيبرانية ذات الدوافع المالية، نبقى ثابتين بالتزامنا بحماية البيئات الرقمية، ونتتبع مشهد التهديدات السيبرانية المتطور عن قرب، ونصمم حلولًا أمنية لإحباط الهجمات بشكل استباقي. ولضمان سلامتك، نشجع بقوة على اعتماد استراتيجية أمن سيبراني قوية تتصدى لهذه التهديدات».

وتوصي كاسبرسكي المستخدمين بعدة إجراءات للوقاية من التهديدات ذات الدوافع المالية، وهي:

عدَّ نسخاً احتياطية لبياناتك لتكون غير متصلة بالإنترنت ولا يمكن للمهاجمين العبث بها. وتأكد من إمكانية الوصول إليها بسرعة عند الحاجة.

ثبِّت حلول الحماية من برمجيات الفدية على جميع النقاط الطرفية، مثل الأداة المجانية، التي تحمي الحواسيب والخوادم من برمجيات الفدية والبرمجيات الخبيثة الأخرى، وتمنع عمليات الاستغلال، وتتوافق مع الحلول الأمنية المثبتة مسبقاً.

استخدم حلاً لحماية النقاط الطرفية وخوادم البريد الإلكتروني يتمتع بقدرات لمكافحة التصيد الاحتيالي، وذلك بهدف تقليل فرصة الإصابة من خلال رسائل التصيد الاحتيالي.

أجرِ تدقيقاً لأمن شبكاتك السيبراني وعالج أي نقاط ضعف تكتشفها في محيط الشبكة أو داخلها.

برمجيات الفدية هي جريمة يعاقب عليها القانون. فإذا وقعت ضحيتها، لا تدفع الفدية أبداً. إذ لن يضمن الدفع استعادة بياناتك، لكنه سيشجع المجرمين على مواصلة أعمالهم. عوضاً عن ذلك، أبلغ عن الحادثة إلى جهات إنفاذ قانون المحلية، وحاول البحث عن برنامج لفك التشفير على الإنترنت.