بينها "الفيس بوك".. باحثون يحذرون من وجود برامج تسرق البيانات الشخصية

الخميس 23 فبراير 2023 12:19 م

حذرباحثو كاسبرسكي من وجود حملة تخريبية مستمرة تقوم على برمجية خبيثة جديدة تستغلّ الشعبية المتزايدة لروبوت الدردشة القائم على الذكاء الاصطناعي ChatGPT.

وقال الباحثيم إن مجرمو الإنترنت بتوزيع البرمجية الخبيثة عبر مجتمعات فيس بوك Facebook، مقدمين نسخة مزيفة من ChatGPT خاصة بالحواسيب المكتبية

ونوهوا إلى أن المستخدمون يتلقون بدل الروبوت، رسائل من شخص يُدعى Fobo يسرق معلومات حساسة مثل بيانات اعتماد تسجيل الدخول إلى حسابات فيس بوك وتيك توك TikTok وجوجل Google، فضلًا عن البيانات المالية الشخصية والشركات

وحدّد باحثو كاسبرسكي الحملة الخبيثة التي تستهدف مستخدمي ChatGPT، روبوت المحادثة القائم على الذكاء الاصطناعي، والذي حظي في الأشهر القليلة الماضية باهتمام عشاق التقنية والمبدعين وغيرهم

وينشئ المحتالون مجموعات على الشبكات الاجتماعية تحاكي بشكل مقنع حسابات شركة OpenAI الرسمية المنتجة لـ ChatGPT، أو تبدو وكأنها مجتمعات للمهتمين بهذا الروبوت

وتنشر هذه المجموعات الاحتيالية منشورات تبدو رسمية وتحتوي على أخبار حول الخدمة وتروّج للبرمجية الخبيثة التي تنتحل شكل النسخة المكتبية من تطبيق ChatGPT.

منشور على وسائل التواصل الاجتماعي يعرض الحصول على حساب ChatGPT تجريبي

ويجري توجيه المستخدمين، بمجرد أن ينقروا على الوارد في المنشور، إلى موقع ويب جيّد التصميم يبدو متطابقًا تقريبًا مع موقع ChatGPT الرسمي، والذي يطلب من المستخدم تنزيل إصدار ChatGPT المزعوم لنظام ويندوز Windows. لكن هذا الإصدار في الواقع ليس سوى أرشيف يتضمّن ملفًا قابلًا للتنفيذ وتبدأ عملية التثبيت لكنها تتوقف فجأة برسالة خطأ تفيد بتعذر تثبيت البرنامج، فيظنّ المستخدم ببساطة أن البرمجية لم يتمّ تنزيلها ولا تثبيتها، فينسى أمرها

ويتم في الواقع استكمال تثبيت التروجان على جهاز المستخدم دون معرفته، قبل أن يثبّت هذا الفيروس رابط آخر، Trojan-PSW.Win64.Fobo، على الجهاز

ووجد خبراء كاسبرسكي أن المهاجمين يستهدفون مختلف أنحاء العالم، إذ هاجمت النسخة المكتبية المزيفة من ChatGPT مستخدمين في إفريقيا وآسيا وأوروبا وأمريكا

ورأت داريا إيفانوفا الخبيرة الأمنية لدى كاسبرسكي أن هذه حملة برمجية ChatGPT الخبيثة تشكل مثالًا واضحًا على سبل تسخير المجرمين أساليب الهندسة الاجتماعية لاستغلال ثقة المستخدمين في العلامات والخدمات الشهيرة وقالت: "على المستخدمين إدراك أن المظهر الرسمي لخدمة ما لا يعني ضمان أنها رسمية وحقيقية، لذلك فإنه ينبغي لهم توخي الحذر والحرص على متابعة المستجدات وحماية أنفسهم من هذه الأنواع من الهجمات".

توصيات خبراء كاسبرسكي للمستخدمين لحماية أنفسهم والتعرّف على التقنيات الجديدة بطريقة آمنة:

توخي الحذر عند تنزيل البرمجيات من الإنترنت، لا سيما إذا كانت من موقع ويب تابع لجهة خارجية، ويبقى من الأَولى عدم تنزيل البرمجيات إلاّ من المواقع الرسمية للشركات أو الخدمات المطورة والمنتجة لها

التحقُّق من سلامة موقع الويب قبل تنزيل البرمجيات منه، من خلال إيجاد رمز القفل في شريط العناوين، والتأكد من أن عنوان URL لموقع الويب يبدأ بالبادئة https://.

استخدام كلمات مرور قوية وفريدة لكل حساب، مع تفعيل ميزة المصادقة الثنائية ما أمكن، للمساعدة في حماية الحسابات من التعرّض للاختراق

الحذر من الروابط أو رسائل البريد الإلكتروني المشبوهة والواردة من مصادر غير معروفة؛ فغالبًا ما يستخدم المحتالون أساليب الهندسة الاجتماعية لخداع المستخدمين ودفعهم للنقر على الروابط أو تنزيل برمجيات خبيثة

استخدام حل أمني موثوق به وضمان تحديثه باستمرار، فالحلّ Kaspersky Premium، مثلًا، يتم تزويده بأحدث المعلومات أولًا بأول للمساعدة في الكشف عن أية برمجيات خبيثة قد تكون على جهاز المستخدم، وإزالتها