حملات تصيد تستهدف مستخدمي النسخة المدفوعة من تيليجرام

16 ديسمبر، 2024

حذرت كاسبرسكي من انتشار عروض مزيفة لخدمة Telegram Premium عالمياً، والتي تستهدف المستخدمين بعمليات خداع تصيدية وبرمجيات خبيثة متنكرة في إصدارات بديلة لتطبيق تيليجرام. تهدف هذه الهجمات لسرقة بيانات اعتماد الحسابات أو اختراق الأجهزة. وتستغل عمليات الخداع شهرة خدمة Telegram Premium وميزة الإهداء، مما يبرز ضرورة يقظة المستخدمين.

خدمة Telegram Premium هي خدمة تقدم اشتراكاً يحتوي على ميزات حصرية لمنصة تيليجرام مثل سرعات تنزيل أسرع، وتحويل الصوت لنص، وملصقات مميزة، وتجربةً خاليةً من الإعلانات، وغيرها. يمكن للمستخدمين إهداء الاشتراك، وهو ما يستغله المحتالون، بجانب ميزات Telegram Premium الأخرى بشكل عام.

خلال موسم العطلات القادم، والذي يشهد تبادل الهدايا وانطلاق الاحتفالات، من الضروري توخي الحذر لتجنب الوقوع ضحيةً لهذه الحيل.

تبدأ إحدى الحيل عندما يتلقى المستخدم رسالةً تبدو وكأنها جاءت من شخص في قائمة جهات الاتصال الخاصة به، والذي يُحتمل أن حسابه قد تعرض للاختراق. تزعم الرسالة قائلةً: «لقد وصلتك هدية: اشتراك بخدمة Telegram Premium». أسفل الرسالة، ثمة رابط يبدو مشروعاً،

والذي يعيد توجيه المستخدم لصفحة تصيدية تحثه على تسجيل الدخول لتطبيق تيليجرام. إذا قام الضحية بمسح الكود أو إدخال بيانات اعتماده، سيتعرض حسابه للاختراق على الفور، مما يمكن المخادعين من الوصول لتفاصيل تسجيل الدخول، وكلمة المرور، وربما كود المصادقة الخاص بهم.

هناك حيل أخرى تتعلق بموضوع خدمة Telegram Premium، والتي يمكن أن تنطلق من مصادر مختلفة بالإضافة لرسائل تطبيق تيليجرام. فقد يستخدم المهاجمون طرقاً أخرى لإرسال روابط تصيدية، مثل البريد الإلكتروني.

على سبيل المثال، يقوم الجناة بإطلاق «مسابقات توزيع هدايا» وهمية لاشتراكات خدمة Telegram Premium. ويتم جذب الضحايا للمشاركة عبر إغرائهم بالجوائز، ليتم توجيههم بعدها عبر مجموعة من الخطوات إلى موقع تصيدي يُطلب فيه منهم إدخال بيانات اعتماد حساباتهم على تطبيق تيليجرام، مما يؤدي في النهاية لاختراق حساباتهم.

مثال لمسابقة توزيع هدايا تصيدية تستغل خدمة Telegram Premium

تشمل الحيل الأخرى قيام المجرمين السيبرانيين بإرسال دعوة للضحايا لتنزيل ملف مضغوط بصيغة ZIP بدعوى أنه يحتوي على نسخة من تطبيق المراسلة مزود باشتراك خدمة Telegram Premium. لكن وفي الواقع، يعيد رابط التنزيل توجيه المستخدمين لصفحة تصيدية يُطلب فيها منهم تسجيل الدخول لتطبيق تيليجرام مرةً أخرى.

مثال لتصيد احتيالي متنكر في عرض لخدمة Telegram Premium

يتضمن احتيال آخر توزيع برمجية خبيثة متنكرة في إصدار بديل من تطبيق تيليجرام مزود باشتراك «مُدمج» لخدمة Telegram Premium. إذ يرسل المخادعون روابطاً للضحايا لتحميل ملفات بصيغة APK، زاعمين أنها إصدارات معدلة من التطبيق، ولكنها في الواقع برمجيات خبيثة.

مثال لصفحة توزع برمجيات خبيثة متنكرة في تطبيق تيليجرام مزود باشتراك خدمة Telegram Premium.

قالت أولجا سفيستونوفا، الخبير الأمني لدى كاسبرسكي: «لوحظت المخططات التصيدية التي تستغل شهرة خدمة Telegram Premium بلغات متعددة، مما يشير لعمل الجناة على مستوى عالمي. حتى وإن لم تصل عمليات الخداع هذه لمنطقة محددة بعد، إلا أن هناك احتمالية للوصول

إليها في النهاية. لذا، يجب توخي الحذر والتشكيك في العروض التي تبدو جيدةً لدرجة يصعب تصديقها، وخاصةً خلال موسم العطلات. وبالإضافة لما سبق، تأكد من تحديث إعدادات الأمن والخصوصية في تطبيق تيليجرام، واحتواء جهازك على حل أمني قوي.»

يستمر المخادعون في تطوير أساليبهم، ويمكن أن تظهر خدع جديدة يومياً. لحماية نفسك من هذه التهديدات، يوصي خبراء كاسبرسكي بما يلي:

• تحقق من دليل كاسبرسكي للحصول على نصائح حول أمن وخصوصية تطبيق تيليجرام.

• تحقق جيداً من الروابط، بما يشمل العناوين الفعلية المخفية ضمن الروابط التشعبية. في بعض الحالات، لاحظت كاسبرسكي احتواء نصوص روابط تشعبية تبدو مشروعة، مثل https://t.me/premium، على عناوين أخرى تختفي خلفها وتعيد توجيه الضحايا لصفحات تصيدية مختلفة تماماً. لذا مرر مؤشر الفأرة فوق الرابط للتحقق من الرابط الفعلي.

• تحقق من الروابط الواردة من جهات الاتصال عبر التأكد من المرسل من خلال قناة تواصل بديلة إذا بدا رابط الهدية مريباً.

• اشترِ الاشتراكات من خلال القنوات الرسمية فقط. على سبيل المثال، يوفر تطبيق تيليجرام روبوتاً خاصاً لشراء اشتراكات خدمة Telegram Premium.

• فعل المصادقة الثنائية (2FA)، فقد تكون هذه آخر خط دفاع، حتى ولو اختُرقت بيانات اعتماد الحساب. يمكن تخزين رموز المصادقة الثنائية بسهولة في تطبيق Kaspersky Password Manager.

• استكشف طرقاً أخرى يستخدمها المجرمون السيبرانيون لسرقة حسابات تيليجرام. إذ يُعد فهم هذه الاحتيالات قبل وقوعها أمراً بالغ الأهمية لتحسين النظافة السيبرانية والبقاء على دراية بالتهديدات المحتملة.

• تجنب تنزيل الإصدارات غير الرسمية من التطبيقات. وتوصي كاسبرسكي بالالتزام بالتطبيقات الرسمية، فقد تحتوي التطبيقات غير الرسمية على أنواع مختلفة من البرمجيات الخبيثة.