الخليج

اقتصاد, تقنية وسيارات

26 أبريل 2024 12:33 مساء

تحذير من تهديدات مخفية بروابط قصيرة تحمل مخاطر خصوصية وأمان

دبي: «الخليج»

أصبحت الروابط القصيرة جزءاً لا غنى عنه في تجربة الإنترنت اليوم. إذ ينقر العديد من المستخدمين على روابط أو سواها من الروابط، التي تم إنشاؤها بواسطة أداة تقصير الروابط دون تردد. ومع ذلك، يمكن (ow.ly) أو (bit.ly) أن تشكل الروابط القصيرة تهديدات كبيرة للخصوصية والأمان، ولو أنها لا تعامل بشكل جدّي في معظم الحالات. وهنا، تشرح «كاسبرسكي» سبب أهمية الحفاظ على اليقظة، وكيف يمكن للأفراد والشركات حماية أنفسهم من الاختراقات المحتملة.

جعلت الروابط القصيرة تصفح الإنترنت، والتواصل عبر تطبيقات المراسلة أسهل وأسرع، وبالأخص على الأجهزة المحمولة. كما يمكن لهذه الروابط تحسين المشاركة على منصات التواصل الاجتماعي، حيث يكون طول الرسائل محدوداً في كثير من الأحيان. يقوم معظم الأشخاص بنسخ الرابط المختصر تلقائياً ولصقه، وتسمح العديد من خدمات تقصير الروابط الشائعة بتخصيص اسم عنوان الويب البديل، الذي يريدون استخدامه. لكن هنا تكمن المشكلة. فعلى عكس الروابط التقليدية، لا تسمح الروابط المختصرة للمستخدم بالتمرير فوقها ومعرفة عنوان موقع الويب الفعلي. لذا، وفي معظم الحالات، لا يمكنك التأكد مما ينتظرك على الطرف الآخر من الرابط المختصر حتى تقوم بالضغط عليه

وزيارته.
وإذا استغل مجرمو الإنترنت ثغرة لا تحتاج النقر على متصفح الويب، فيمكن أن تحدث الإصابة بمجرد وصول المستخدم إلى موقع الويب الخبيث. كما يمكن لهؤلاء المجرمين استخدام أدوات تقصير الروابط، لتغيير العنوان المستهدف حسب الحاجة. فعلى سبيل المثال، إن أرسل المهاجمون رسائل تصيد احتيالي مُرفقة مع رابط، لكن هذا الرابط يقود إلى صفحة هبوط على موقع محظور، لن تكون إعادة استضافته في عنوان مختلف مشكلة، إذا استخدموا أدوات تقصير الروابط للروابط المرسلة من قبلهم. وفي كثير من الأحيان، يتم استخدام عمليات إعادة توجيه متعددة لإخفاء الأدلة التي تقود إلى الرابط الأصلي.
تسمح بعض أدوات تقصير الروابط بتتبع عدد النقرات على الرابط من مكان نشره، ومن حيث المبدأ، يعد ذلك هجوم وساطة، إذ تمر البيانات عبر عقدة خدمة وسيطة تراقب جميع البيانات المتبادلة بين المستخدم والموقع المطلوب. وبالتالي، يمكن لأداة تقصير الروابط اعتراض بيانات الاعتماد المدخلة ورسائل الشبكات الاجتماعية وما إلى ذلك. وعلاوة على ذلك، يمكن استخدام هذه روابط للتشهير وأنواع أخرى من التتبع، خاصةً إذا كانت خدمة تقصير الروابط تُوفّر وظائف متقدمة.
في معظم الحالات، يتم وضع الروابط القصيرة المخصصة للاستخدام العام في منشورات الشبكات الاجتماعية أو على صفحات الويب. ولكن تنشأ مخاطر إضافية، إذا تم إرسال أحدها إلى المستخدم شخصياً، عبر رسالة فورية أو رسالة بريد إلكتروني، إلى عنوان شخصي أو عنوان عمل. وباستخدام هذه الروابط، يمكن للمهاجم (الذي جمع بعض المعلومات حول المستخدم مسبقاً)، إعادة توجيه الضحية المحتملة إلى موقع تصيد احتيالي يتضمن بعض البيانات الشخصية المملوءة مسبقاً. وعلى سبيل المثال، يمكن توجيه الضحية إلى نسخة من موقع مصرفي تتضمن اسم المستخدم الحقيقي الخاص به، وتطلب إدخال كلمة المرور، أو يمكن توجيهه إلى «بوابة دفع»، لخدمة ما مع ملء رقم بطاقة مصرفية شخصية بشكل مسبق، والاكتفاء بطلب إدخال رمز الأمان من المستخدم.
بالنظر إلى مدى شيوعها وسهولة استخدامها، لا يعد تجنب النقر على الروابط المقصرة خياراً حقيقياً. في أغلب الأحيان، يتم استخدام أدوات تقصير الروابط لأغراض مشروعة وآمنة تماماً. لكن وعلى الرغم من ذلك، يعني وجود مصادر تهديد تتطلع إلى استغلال ثقة الأشخاص في الخدمة، أن يقظة المستخدم مهمة. وفي حالة العثور على رابط مثير للشك في رسالة مُعاد توجيهها، أو من عنوان بريد إلكتروني غير مألوف، أو جهة اتصال غير معروفة، فالطريقة السهلة لفحصه، هي نسخه ولصقه في أداة من أدوات الحماية. كما يمكن للمستخدمين اختيار تثبيت حل أمان مثل «كاسبرسكي بريميوم» للأجهزة الشخصية، بينما يمكن للمؤسسات اختيار مستوى يناسبهم من خدمة «كاسبرسكي نيكست»، إذ تحذر هذه الحلول المستخدم، قبل أن يجد نفسه في موقع ويب خطير، وتقوم بذلك حتى لو كان الرابط مقصراً. كما أنها تحمي أجهزتك من أي محاولات إصابة، بما يتضمن الهجمات التي تستغل نقاط ضعف غير مكتشفة بعد.
وقال سيف الله جديدي، الرئيس الإقليمي لأعمال المستهلكين في «كاسبرسكي»: «إن أفضل الدفاعات ضد التهديدات الإلكترونية، التي قد تشكلها الروابط المختصرة هي حل أمني شامل مقترن بوعي المستخدمين ويقظتهم. إذ تنتج العديد من خروقات الأمن السيبراني عن الأخطاء البشرية وتقنيات الهندسة الاجتماعية، لذلك يجب على الناس إبقاء أنفسهم على اطّلاع، بينما يجب على المؤسسات التفكير في برامج تعليمية منتظمة مثل (Kaspersky Automated Security Awareness Platform) لتزويد الموظفين بالمعرفة والمهارات اللازمة لحماية بيانات الشركة ومعلوماتها الحساسة من القرصنة، أو التصيد الاحتيالي، أو غيرها من الانتهاكات».