الخليج

اقتصاد, تقنية وسيارات

5 سبتمبر 2022 13:59 مساء

مع قرب إطلاق «آيفون 14».. محتالون يستهدفون المهتمين بأحدث هواتف «أبل»

عثر خبراء كاسبرسكي على العديد من صفحات التصيّد التي تعرض على المهتمين شراء هاتف «أبل» المرتقب الجديد «آيفون 14»، بعدما أكّدت أن الهاتف سيُطرح، الأربعاء، 7 سبتمبر/ أيلول 2022 خلال حدثها السنوي العالمي. وانما تلك الصفحات الوهمية سوى فخاخ مصمّمة للإيقاع بالمستخدمين وسرقة حساباتهم المصرفية وبيانات الدخول إلى حساباتهم على «أبل». ونجحت حلول أمن كاسبرسكي بين 10 و25 أغسطس الماضي في اكتشاف أكثر من 8700 صفحة تصيّد جديدة متعلقة بطرح الهاتف «آيفون 14».

وارتفع عدد صفحات التصيّد المتعلقة بـ «آيفون 14» والتي تظهر كلما اقترب موعد طرحه. واكتشف خبراء كاسبرسكي في يوم 25 أغسطس وحده، مثلاً، ما مجموعه 1023 صفحة تصيّد متعلقة بالهاتف الجديد، أي نحو ضِعف متوسط عدد الصفحات المكتشفة يومياً في المدّة المذكورة.

عدد صفحات التصيّد

وينشئ مجرمو الإنترنت كالعادة، قبيل طرح أي هاتف «آيفون» جديد في السوق، صفحات مزيفة تحاكي متاجر إلكترونية تعرض فرصة حجز الهاتف الجديد مسبقاً بسعر مخفض أو حتى شرائه قبل الإعلان الرسمي. ويستخدم المحتالون صوراً لهواتف قديمة من «أبل» لجذب انتباه المستخدمين، في ظلّ انعدام الصور الرسمية للهاتف 14 الجديد على الإنترنت. ويخسر المستخدم الضحية المال بعد أن يُدخل بيانات بطاقته المصرفية لدفع ثمن الهاتف المزعوم، الذي لن يتلقاه بالطبع.

صفحة تصيد بالفيتنامية

لا يقتصر اهتمام مجرمي الإنترنت بشعبية أجهزة «آيفون» على إصدار هواتف الجديدة، وإنما يسعون أحياناً وراء الحصول على معرّفات «أبل» والوصول إلى خدمات الشركة مثل App Store وApple Music وiCloud وغيرها. ويحاول المحتالون خداع ضحاياهم ودفعهم إلى إدخال اسم المستخدم وكلمة FaceTime وiMessage والمرور الخاصة بحسابهم على «أبل» في صفحة تصيّد خاصة مزيفة يُنشئونها لهذا الغرض، ما يمكّنهم من الوصول إلى عناوين البريد الإلكتروني كلمات المرور الخاصة بضحاياهم، بالإضافة إلى جهات الاتصال ومعلومات الدفع. ويمكن لمجرمي الإنترنت أيضاً عبر هذا الاختراق الوصول إلى خدمة «آي كلاود» الخاصة بالضحية، حيث يحفظ المستخدمون صورهم ومستنداتهم الشخصية. وقد يستخدم المهاجمون هذه الصور لاحقاً لانتحال الهوية الشخصية أو الابتزاز.

«استخدام معرِّف «أبل

وقد يضغط المحتالون على الضحايا من أجل الوصول إلى معرِّف «أبل» الخاص بهم عبر إبلاغهم بأنهم قد يفقدون القدرة على استخدام أجهزتهم في أية لحظة بسبب بعض التهديدات. فمثلًا، وجد خبراء كاسبرسكي صفحات تصيّد تظهر فجأة على شاشة الجهاز محذّرة الضحايا من أن «الوصول إلى هذا الجهاز قد حُظر بسبب أنشطة غير قانونية»، وأن عليهم من أجل استعادة الوصول إلى الجهاز، الاتصال برقم دعم مزيف تابع لشركة «أبل»، وفق زعمهم. وتُدعى محاولات الاحتيال هذه بـ «التصيد الصوتي»، حيث يجري إقناع الضحية بالاتصال بالمحتالين هاتفياً والكشف لهم عن البيانات الشخصية والتفاصيل المصرفية. وبوسع هذه الصفحات «قفل» شاشة الحاسوب، وعرض رسالة التهديد فقط بحيث لا يكون لدى المستخدم خيار سوى الاتصال بالرقم الذي يقدّمه المحتالون، الذين يلجأون أثناء المكالمة إلى العديد من أساليب الهندسة الاجتماعية للحصول من ضحاياهم على بيانات معرِّفات «أبل» ومعلوماتهم الشخصية، وتفاصيل بطاقة الائتمان للحصول على رسوم الدعم عبر الهاتف.

صفحة متابعة مع تحذير

وقالت أولغا سفيستونوفا خبيرة الأمن لدى كاسبرسكي، إن مجرمي الإنترنت غالباً ما يراقبون التوجّهات الجديدة بنشاط أكبر من نشاط المستخدمين العاديين، ويبحثون باستمرار عن موضوع جذّاب يثير اهتمام الأفراد، ويمكن استخدامه كطعم لخداعهم ودفعهم لإدخال بيانات الدخول إلى الحسابات الشخصية أو بيانات الدفع. وأضافت: «يُعدّ طرح هواتف آيفون الجديدة من المواضيع المثيرة لاهتمام الأفراد، لذلك نرى نشاطاً متزايداً لمجرمي الإنترنت في المدة التي تسبق الإصدار السنوي لهذا الهاتف الذكي. ولهذا السبب يجب على المستخدمين توخّي الحذر والامتناع عن إدخال بياناتهم الشخصية على الصفحات المشبوهة لتجنب الوقوع ضحايا لمجرمي الإنترنت».

توصيات

وتوصي كاسبرسكي المستخدمين باتباع التدابير التالية لتجنب الوقوع ضحية لعمليات الاحتيال:

- التحقُّق من صحة موقع الويب قبل إدخال البيانات الشخصية، وعدم اللجوء إلا إلى صفحات الويب الرسمية وتهجئة اسم URL والموثوق بها لمشاهدة الأفلام وتنزيلها، مع ضرورة التحقُّق جيداً من تنسيقات عناوين الشركة.
- يُفضّل تجنُّب النقر على الروابط الواردة في رسائل البريد الإلكتروني عموماً. ويمكن بدلاً من ذلك فتح علامة تبويب أو نافذة جديدة في المتصفح وإدخال عنوان البنك أو الجهة المفترض أن يوصلني الرابط إليها، يدوياً.
- تجنُب تسجيل الدخول إلى الخدمات المصرفية الرقمية والخدمات المماثلة من خلال شبكات إنترنت لاسلكية عامة، بالرغم من كونها طريقة ملائمة للاتصال، ولكن من الأفضل دائماً استخدام شبكات آمنة. إذ يمكن إنشاء الشبكات المفتوحة من قبل المجرمين الذين قد يسرقون عناوين مواقع الويب عبر الاتصال، وبالتالي يوجّهون المستخدم إلى صفحة مزيّفة.
- استخدم حلاً أمنياً موثوقاً يحدّد المرفقات الخبيثة ويحظر مواقع التصيّد.