في 2021 اللص ليس بحاجة لكسر قفل..تعرفوا وسائل النصب الحديثة!



وجه الخبير في أمن المعلومات في شركة "كاسبيرسكي"، المبرمج "دميتري غالوف"، التحذير من بعض الأساليب التقنية التي باتت تستخدم للإحتيال على الناس في السنوات الأخيرة ، إذ أصبحت الجرائم الإلكترونية من أشهر وأخطر وسائل النصب في زماننا هذا.

خدعة الاتصال المزيف:

من أبرز أساليب الجرائم المالية الإلكترونية، وفقًا للخبير هو عندما يقوم أحد المحتالين بالاتصال بضحيته وينتحل شخصية موظف في المصرف الذي يتعامل معه المستهدف، ثم يطلب منه معلومات تتعلق بالبطاقة المصرفية بحجة إيقاف معاملات مالية مشبوهة، وبعد حصول المحتال على بيانات البطاقة يقوم باستغلالها لسرقة وتحويل الأموال إلى حسابات تخصه.

وقال غالوف: "هذه الطريقة من الاحتيال انتشرت على نحو واسع في روسيا عامي 2013 و2014، لكنها عادت للظهور بوضوح هذا العام، وبات المحتالون يملكون الكثير من البيانات المصرفية للضحايا، وربما

تعلموا استغلال تلك البيانات بشكل أكبر من قبل".

خدعة الرسالة الخبيثة:

الأسلوب الآخر الذي أشار إليه الخبير هو الاحتيال عبر الإنترنت، وتحديداً عبر تطبيقات المحادثة والتواصل الاجتماعي. فعندما تتلقى الضحية رسالة فيها رابط إلكتروني خبيث، ويطلب نص الرسالة من الضحية الضغط على الرابط للوصول إلى موقع معين أو للتصويت على استفتاء ما، فسيتمكن المحتال بمجرد دخول الضحية إلى هذا الرابط وتفاعلها مع محتواه من اختراق الجهاز أو الحصول على صلاحيات معينة تتيح له الاطلاع على معلومات هامة وحساسة. والأمر هنا متعلق باستجابة الضحية واحترافية المخترق، فهذا النوع من الاختراق له تشعبات عديدة لا يتسع المجال لذكرها.

وهناك طريقة يتبعها بعض المحتالون تحدث عنها الخبير، هي عندما يرسل المحتالون لضحاياهم رسائل معينة تطلب منهم تحويل مبالغ مالية صغيرة كرسوم اشتراك في سحب على جوائز ذات قيمة مادية كبيرة، وتقوم الضحية بتحويل الأموال للمحتال بملء إرادتها.

الاحتيال ثلاثي الأبعاد:

جاءت هذه التسمية بسبب ارتباطه بثلاثة عناصر: الضحية، والموقع المزيف، والبيانات المالية للرصيد البنكي.

عن طريق توافر العناصر المطلوبة يستطيع المحتال جذب الضحية عبر العديد من العروض المغرية على متجره الإلكتروني. وبمجرد أن تقوم الضحية باتخاذ قرار بشراء المنتج، يتمكن المحتال من السيطرة على الحساب الائتماني التابع للمستخدم، واستغلاله كما يشاء.

أو قد يتم استخدام المواقع المزيفة من أجل عقد صفقات شراء تبدو نظامية لكنها تقدم منتجات مزيفة أو لا تقدم شيء على الإطلاق، كأن يقوم البائع بإرسال لعبة هاتف لعميل طلب شراء هاتف ذكي.

الاحتيال الودي أو المسالم:

هي عملية يظهر فيها المحتال وكأنه الضحية وليس الجاني، حيث يقوم بشراء بعض المنتجات عبر متاجر

إلكترونية، وبمجرد أن يتم خصم المبلغ من رصيده البنكي، يقوم بالاتصال اعتراضًا على عملية الخصم، مدعيًا أن بطاقاته الائتمانية قد تعرضت للسرقة.

و تتطلب هذه الطريقة احترافية شديدة حتى ينجح المحتال في إقناع المتجر الإلكتروني والبنك بتعرض حسابه للسرقة، ويتمكن من استرداد المال المدفوع بجانب احتفاظه بالبضائع.

كيف أحمي نفسي من الجرائم الإلكترونية وعمليات النصب؟

لا تشارك بياناتك الائتمانية مع أي شخص حتى لو طلب منك التاجر أو المندوب.

تأكد من الموقع الذي قمت بزيارته عن طريق إضافة عنوانه في موقع net.is who لمعرفة تاريخه وجوده في الإنترنت والمعلومات المتوفرة عنه.

تأكد أن الموقع الذي تتعامل معه آمن عن طريق النظر إلى عنوانه والتحقق من وجود https في مقدمته.

تابع تقييمات العملاء حول المتجر الإلكتروني وحول معاملات الشراء نفسها.

اقرأ مواصفات المنتج جيدًا وتأكد أنها تطابق الصورة المعروضة، وما سيتم استلامه.

قم بقراءة شروط الخصوصية التابعة للموقع وتأكد أنها لا تحتوي على أي بند فيه انتهاك لبياناتك.

قم بطرح الأسئلة على فريق الدعم التابع للموقع وتأكد أنهم خبراء كفاية في الإجابة على كافة أسئلتك.

احذر من المواقع ذات التصميم الرديء والمحتوى الضعيف والصور منخفضة الجودة، فهي في الغالب مواقع مزيفة تم إنشاؤها لهدف مؤقت وهو استغلال الضحايا.

احذر من البائع الذي يصر على ضرورة الدفع الفوري أو الإلكتروني بدون توفير ضمانات الاسترجاع أو المعاينة.