الهواتف الذكية "حصان طروادة" للبرمجيات الخبيثة

12 مارس، 2025

يحتل أمن الهواتف الذكية، المعرضة لأنواع شتى من الهجمات وعمليات الاحتيال، موقعا مركزيا على قائمة المخاوف المرتبطة بقطاع الاتصالات والأجهزة المحمولة الذي يعقد مؤتمره السنوي الأبرز عالميا في برشلونة هذا الأسبوع.

وعشية افتتاح المعرض، قدمت شركة "هونور" الصينية أداة جديدة ستُدمج قريبا في هواتفها الذكية تتيح للمستخدمين بنقرة بسيطة على أيّ مقطع فيديو يتلقونه أن يطلبوا من الجهاز التحقق من صحة الفيديو.

وبفضل الذكاء الاصطناعي، وبعد عملية مسح سريعة، يشير الهاتف، بدقة في التشخيص تبلغ بحسب الشركة 99 في المئة، إلى ما إذا كان مقطع الفيديو حقيقيا أم مزيفا بتقنية "التزييف العميق". ويصعب على الشخص غير الخبير في الموضوع اكتشاف هذه الفيديوهات الواقعية للغاية، والتي يتم إنشاؤها باستخدام الذكاء الاصطناعي.

وعمدت الجمعية العالمية لمشغلي الاتصالات، وهي الجهة المنظمة لهذا الحدث السنوي في عاصمة إقليم كاتالونيا، إلى تطوير "سكام سغنال ""إشارات الاحتيال"، وهي واجهة برمجة (API) مصممة لحماية المستخدمين من الاحتيال المصرفي عبر الهاتف.

وصُممت هذه الواجهة، بالشراكة مع هيئة "يو كاي فاينانس" الناظمة للقطاع المالي في بريطانيا، لمكافحة المكالمات الاحتيالية التي تشجع المستهلكين على الموافقة على المدفوعات على تطبيقهم المصرفي من خلال كشف بعض البيانات، مثل طول المكالمة، في وقت إجراء معاملة مصرفية.

ويسمح هذا للبنوك، في حالة الشك، بـ"حظر المعاملة، والتحقق من أن الأمور تسير بشكل طبيعي، قبل التثبت من صحة التحويل،" على ما توضح مديرة الأمن في سامانثا كيت.

الاحتيال يستخدم قنوات متعددة لتظل الهواتف الذكية محمية بشكل سيء، ما يكفي لجعل هذه الأجهزة المهمة أهدافا رئيسية

ولكن في حين جرى اعتماد مثل هذه الحلول من جانب مشغلي الاتصالات في المملكة المتحدة، فإن الاحتيال يستخدم أيضا قنوات أخرى، وتظل الهواتف الذكية محمية بشكل سيء، ما يكفي لجعل هذه الأجهزة المهمة في الحياة اليومية أهدافا رئيسية.

ووفقا لشركة الأمن السيبراني "كاسبيرسكي"، فإنّ الاحتيال في تطبيقات الخدمات المصرفية هو الذي شهد أكبر نمو بين مختلف أنواع الهجمات الإلكترونية على الأجهزة المحمولة في عام 2024.

وبحسب تقريرها السنوي عن حالة التهديدات عبر الهواتف المحمولة، الذي نشرته بمناسبة المؤتمر العالمي للأجهزة المحمولة في برشلونة، فإن هجمات سرقة البيانات المصرفية على الهواتف الذكية عبر ما يُعرف بـ"أحصنة طروادة"، أي "البرمجيات الخبيثة المصممة لسرقة بيانات اعتماد المستخدمين المتعلقة بالخدمات المصرفية عبر الإنترنت،" تضاعفت ثلاث مرات في عام واحد.

وتكشف هذه الزيادة عن ضعف المستخدمين أمام التطبيقات التي تخفي في بعض الأحيان برمجيات ضارة.

وفي معظم حالات الاحتيال المصرفي، يثبّت المستخدمون تطبيقا ضارا على أجهزتهم المحمولة، بحسب المحلل في فريق البحث والتحليل

الدولي في "كاسبيرسكي" مارك ريفيرو.

ويقول ريفيرو "على سبيل المثال، يريدون تثبيت لعبة، يجدون رابطا على الإنترنت (…) ويحمّلون التطبيق. يبدو التطبيق رسميا، لكنه مزيف، ويتم تثبيت البرنامج الخبيث على الجهاز".

ولا يقتصر التهديد على الروابط الموجودة على شبكة الإنترنت، إذ تحتوي متاجر التطبيقات الرسمية، والتي تأتي مثبتة مسبقا على الهواتف وهي أكثر أمانا، على عيوب في بعض الأحيان.

ومع ذلك، هناك فرق كبير اعتمادا على أنظمة التشغيل للهواتف الذكية، أي خصوصا أندرويد من غوغل ، أو "اي أو أس" بالنسبة إلى هواتف "آي فون". وفي ما يتعلق بالأخير، تظل التطبيقات الخبيثة نادرة للغاية، بحسب تأكيد الكثير من الخبراء.

وبالنسبة إلى مديرة المنتجات في شركة براديو المتخصصة في الأمن السيبراني للهواتف الذكية روكسان سوو، فإن الخطر يتعزز بسبب تهديدات غير مرئية تقريبا.

وتقول "عندما لا تكون الهواتف محمية (بأداة للأمن السيبراني)، فإننا لا نرى ما إذا كان شخص ما قد نقر على رابط التصيد أو حمّل برامج ضارة، لذا فمن الصحيح أنه لا يوجد وعي كبير بين عامة الناس".

لكن الخبيرة تقارب الموضوع بحذر، إذ تشير إلى أن مستوى المخاطر التي تتعرض لها الهواتف يعتمد إلى حد كبير على المعايير التي يحددها المستخدم.

وبالإضافة إلى اليقظة بشأن التطبيقات التي يتم تنزيلها، تنصح سوو بعدم ترك وظيفة البلوتوث مشغّلة بشكل دائم، وإلغاء تنشيط الاتصال التلقائي بشبكة الانترنت اللاسلكي وتحديد المستخدم الشبكة التي يريد الاتصال بها يدويا، وتحديث الجهاز قدر الإمكان.