Judy برمجيات ضارة محتمل وصولها إلى 36.5 مليون مستخدم أندرويد

الاثنين 29 مايو 2017 10:05 م

اكتشف الباحثون ضمن شركة الأمن والحماية "تشيك بوينت" Check Point حملة برمجيات خبيثة واسعة النطاق على متجر برمجيات أندرويد الرسمي المسمى جوجل بلاي، ويطلق على هذه البرمجيات الضارة اسم Judy "جودي"، وهي من نوع برمجيات adware تلقائية النقر، فيما قد يعتبر بحسب تشيك بوينت أكبر حملة برمجيات خبيثة وجدت على متجر جوجل بلاي.

وعثرت الشركة على تلك البرمجية Judy ضمن 41 تطبيقاً جرى نشرهم من قبل شركة كينيويني Kiniwini التي تتخذ من كوريا مقراً لها، ونشرت تحت اسم شركة إنيستوديو كورب ENISTUDIO Corp، حيث تستعمل تلك البرمجيات الضارة الأجهزة المصابة لتوليد كميات كبيرة من النقرات الاحتيالية على الإعلانات، مما يولد إيرادات للأشخاص الذين يقفون خلفها.

وقد حصلت تلك التطبيقات الخبيثة على معدل انتشار كبير يصل بين 4.5 مليون و18.5 مليون عملية تنزيل، وأوضحت الشركة أن عدداً من تلك التطبيقات قد تواجد لسنوات ضمن متجر جوجل بلاي وجرى تحديثها مؤخراً، ومن غير الواضح الفترة الزمنية التي تواجدت فيها الشيفرة البرمجية الخبيثة ضمن تلك التطبيقات، وبالتالي فإن الانتشار الفعلي للبرمجيات الضارة غير معروف.

كما وجدت الشركة العديد من التطبيقات التي تحتوي على البرمجيات الضارة، والتي تم تطويرها من قبل مطورين آخرين على متجر جوجل بلاي، ولا تزال العلاقة بين الحملتين غير واضحة، حيث قد تكون إحدى الحملتين قد استعارت الشيفرة البرمجية الخبيثة من الأخرى عن علم أو دون علم.

وجرى تحديث أقدم تطبيقات الحملة الثانية آخر مرة في شهر أبريل/نيسان 2016، مما يعني أن الشيفرة البرمجية الخبيثة قد تواجدت لفترة طويلة على متجر جوجل بلاي دون الكشف عنها، مما يعني أن الانتشار الكلي للبرمجيات الضارة قد وصل إلى ما بين 8.5 مليون و36.5 مليون مستخدم.

وتعتمد برمجيات "جودي" Judy، وعلى غرار البرمجيات الضارة الأخرى التي وجدت ضمن متجر جوجل بلاي مثل FalseGuide وSkinner، على التواصل مع خادم القيادة والتحكم C&C لتشغيلها، وجرى إزالة هذه التطبيقات بسرعة من متجر جوجل بلاي بعد إبلاغ شركة تشيك بوينت جوجل عن هذا التهديد.

وتعمل شركة Kiniwini على تطوير برمجيات لنظامي تشغيل الأجهزة المحمولة أندرويد وآي أو إس iOS، وتشير شركة الأمن والحماية إلى أنها لم تلاحظ وجود أي مشاكل مع تطبيقات نظام آي أو إس، ويتواجد 45 تطبيقاً من شركة ENISTUDIO Corp ضمن متجر تطبيقات آبل، ويبدو أن آخر تحديث لمعظمها تم في 31 مارس/آذار الماضي.