اسيت: فيروسات خطيرة لسرقة الأموال تستغل متجر جوجل بلاي

الخميس 28 سبتمبر 2017 04:09 م

كشفت شركة اسيت Eset أن موجة جديدة من برمجيات حصان طروادة الخطيرة المتخصصة بسرقة الحسابات المصرفية والعاملة على نظام التشغيل أندرويد نجحت مجددًا في الدخول إلى متجر جوجل بلاي مسلحةً بأساليب وتقنيات جديدة، وذلك بعد أن حذرت الشركة من خطورة هذه البرمجيات في بداية هذا العام.

وقالت الشركة المتخصصة في أمن المعلومات أن البرمجية الخبيثة المسماة "بانكبوت" BankBot قد واصلت تطورها خلال العام الحالي لتظهر بأشكال ونسخ مختلفة داخل متجر جوجل بلاي وخارجه.

وأضافت الشركة السلوفاكية أن النمط الجديد من حصان طروادة والذي اكتشفته في المتجر بتاريخ 4 أيلول/سبتمبر يعد أولى تلك البرمجيات الخبيثة التي تدمج أحدث خطوات تطور برمجية "دوبت بانكبوت" بشكل ناجح؛ إذ تم تحسين أنماط تشفير البيانات، وتعزيز دقة تفريغ حمولة البيانات، إلى جانب الاستعانة بتقنيات ماكرة لنقل البرمجيات عبر استغلال صلاحيات الوصول في نظام تشغيل أندرويد.

وذكرت اسيت أن حالات استغلال صلاحيات الوصول لنظام تشغيل أندرويد باستخدام عدد من برمجيات حصان طروادة سُجلَّت خارج متجر جوجل بلاي في معظم الأحيان. وأكدت التحليلات التي صدرت حديثًا عن شركتي "إس فاي لابس" SfyLabs و "زد سكيلر" Zscaler أن قراصنة الإنترنت الذين يعملون على نشر "بانكبوت" قد نجحوا في رفع التطبيق من خلال استغلال صلاحيات الوصول الخاصة بمتجر جوجل بلاي، من دون تضمينه حمولة بيانات البرمجيات الخبيثة الخاصة بالسرقات المصرفية.

ويتمثل حل هذا اللغز في أن حمولة بيانات البرمجية الخبيثة قد تمكنت من الانسلال متجر جوجل بلاي بشكل لعبة تحمل اسم "جويلز ستار كلاسيك"Jewels Star Classic (وتجدر الإشارة هنا إلى أن القراصنة أساؤوا استخدام الاسم الشهير لإحدى منصات الألعاب المشروعة "جويلز ستار"Jewels Star المطورة من قبل شركة "آي تري جيمر" ITREEGAMER والتي لا ترتبط على الإطلاق بهذه الهجمة البرمجية الخبيثة).

وقالت شركة اسيت إنها قامت بإبلاغ الفريق الأمني لشركة جوجل بشأن هذا التطبيق الخبيث، والذي تم تنزيله من قبل نحو 5 آلاف مستخدم قبل أن يقوم المتجر بإزالته.

كيف تعمل هذه البرمجية الخبيثة؟

أوضحت الشركة أنه حينما يقوم المستخدم غير المنتبه بتنزيل لعبة "جويلز ستار كلاسيك" – المطوّرة من قبل "جيمدف توني" GameDevTony، فإنه يحصل على لعبة يمكن تشغيلها على نظام أندرويد. وباستخدام بعض الإضافات المخفية، يمكن للقرصان تشغيل حمولة البيانات الخبيثة الكامنة داخل اللعبة، إلى جانب خدمة خبيثة يتم تفعيلها بعد مهلة معينة تم تحديد مدتها خلال وقت سابق.

ويتم تشغيل الخدمة الخبيثة بعد مرور 20 دقيقة على التشغيل الأول للعبة "جويلز ستار كلاسيك". وبعدها يقوم الجهاز المصاب بالبرمجية الخبيثة بعرض تنبيه يطالب المستخدم بتمكين خدمة تحمل اسم "خدمة جوجل"Google Service (ملاحظة: يظهر التنبيه بشكل مستقل عن النشاط الحالي للمستخدم، ودون أي علاقة ظاهرة له مع اللعبة).

وبعد ضغط المستخدم على خيار "موافق"، والذي يمثل السبيل الوحيد لمنع التنبيه من الظهور مجددًا، ينتقل المستخدم تلقائيًا إلى قائمة الوصول الخاصة بنظام أندرويد، حيث تتم إدارة صلاحيات الوصول في النظام. وتظهر بين مجموعة الخدمات المشروعة خدمة جديدة تسمى "خدمة جوجل" التي أنشأتها البرمجية الخبيثة. ومن خلال الضغط على هذه الخدمة يتم عرض وصف مأخوذ عن اتفاقية "شروط استخدام الخدمة" الخاصة بشركة جوجل.

وحينما يقرر المستخدم تفعيل الخدمة، تظهر لديه قائمة من الصلاحيات التي يتعين عليه منحها وتشمل: "راقب نشاطاتك"، و"استعادة نافذة المحتوى"، و"تفعيل الاستكشاف من خلال اللمس"، و"تفعيل الوصول المحسّن إلى الشبكة"، و"تنفيذ الإجراءات".

وبمجرد الضغط على زر "موافق"، يتم منح صلاحيات الوصول الخاصة بالبرمجية الخبيثة. ومن خلال منح هذه الصلاحيات، فإن المستخدم يمنح البرمجية الخبيثة حرية كاملة في تنفيذ جميع الإجراءات التي تحتاجها لمواصلة أنشطتها الخبيثة.

ومن الناحية العملية وبعد الموافقة على منح الصلاحيات، يتم منع وصول المستخدم لفترة قصيرة إلى شاشة جهازه المحمول ريثما تتم "ترقية خدمة جوجل"Google service update – وتجدر الإشارة هنا أن "جوجل" لا تتولى إدارة هذه العملية.

وتستخدم البرمجية الخبيثة هذه الواجهة على الشاشة للتغطية على خطواتها التالية، وتفعيل العمليات نيابة عن المستخدم من خلال الاستعانة بأذونات الوصول التي حصلت عليها البرمجية الخبيثة خلال وقت سابق. وبينما ينتظر المستخدم انتهاء تحميل الترقية الوهمية، تقوم البرمجية الخبيثة بتنفيذ عدد من العمليات.

ومن تلك العمليات السماح بتحميل التطبيقات من مصادر مجهولة، وتثبيت برمجية "بانكبوت" الخبيثة من مصدرها وتفعيلها، وتفعيل "بانكبوت" كمسؤول إدارة الجهاز، وتعيين "بانكبوت" كتطبيق افتراضي للرسائل القصيرة، والحصول على أذونات لتحميل المزيد من التطبيقات الأخرى.

وبعد نجاحها في تنفيذ هذه العمليات، يصبح بإمكان البرمجية الخبيثة البدء بالعمل على تحقيق هدفها التالي والمتمثل بسرقة معلومات بطاقة الائتمان الخاصة بالمستخدم. وبعكس برمجيات "بانكبوت" الأخرى التي تستهدف مجموعة واسعة من التطبيقات المصرفية المحددة والتي تنتحل أشكالها بهدف الحصول على بيانات الاعتماد الخاصة بالدخول إلى الحسابات المصرفية، ينصب تركيز هذه البرمجية بشكل أساسي على تطبيق جوجل بلاي المثبت على جميع الأجهزة العاملة بنظام تشغيل أندرويد.

وعندما يقوم المستخدم بتشغيل تطبيق جوجل بلاي، تتدخل برمجية "بانكبوت" لتكتسي بالطابع الشرعي للتطبيق وتستخدم نموذجًا مزيفًا منه لطلب معلومات بطاقة الائتمان الخاصة بالمستخدم.

وفي حال انطلت خدعة النموذج المزيف على المستخدم وقام بإدخال معلومات بطاقته الائتمانية، يكون القراصنة قد نجحوا في تحقيق مسعاهم الأساسي. ونظرًا لنجاح برمجية "بانكبوت" في تعيين نفسها كتطبيق افتراضي للرسائل القصيرة، فقد بات بإمكانها اعتراض جميع الرسائل القصيرة المتبادلة على الجهاز المصاب. ويتيح ذلك للقراصنة القدرة على تجاوز أنظمة المصادقة الثنائية الخاصة بالحساب المصرفي الخاص بالمستخدم، والتي تمثل آخر العقبات المحتملة التي تحول بينهم وبين أموال المستخدم.

ما هي أسباب الخطورة العالية لهذه الهجمة الإلكترونية؟

يمزج القراصنة في هذه الهجمة الإلكترونية مجموعة واسعة من التقنيات ذات الشعبية المتنامية بين مصممي البرمجيات الخبيثة على نظام تشغيل أندرويد والتي تشمل استغلال صلاحيات الوصول على نظام أندرويد، وانتحال شكل تطبيقات "جوجل"، وإعداد مؤقت زمني لتأخير بدء نشاط البرمجية الخبيثة بهدف تجنب إجراءات "جوجل" الأمنية.

وتسهم هذه التقنيات مجتمعة في جعل إمكانية اكتشاف التهديد في الوقت المناسب أمرًا بالغ الصعوبة بالنسبة للمستخدم. ولأن البرمجية الخبيثة تنتحل شكل تطبيقات "جوجل" وتنتظر 20 دقيقة قبل عرض التنبيه الأول، تتضاءل فرصة المستخدم في الربط بين أنشطتها وبين تطبيق "جويلز ستار كلاسيك" الذي قام بتحميله مؤخرًا. علاوة على ذلك، تسهم الأسماء والأشكال المختلفة التي تستخدمها البرمجية الخبيثة خلال مختلف مراحل إصابة الجهاز في تعقيد الجهود المبذولة لتحديدها وإزالتها بشكل يدوي.

كيفية إزالة البرمجية الخبيثة عن الأجهزة المصابة؟

يتعين على المستخدمين الذين يقومون بتحميل الكثير من التطبيقات من متجر جوجل بلاي وغيره من المتاجر الأخرى التحقق من عدم وجود هذه البرمجية الخبيثة.

ولا يعد فحص الجهاز للتأكد من عدم وجود لعبة "جويلز ستار كلاسيك" إجراءًا كافيًا، إذ غالبًا ما يقوم القراصنة بتغيير التطبيقات التي يستخدمونها لنشر برمجية "بانكبوت".

ولمعرفة فيما إذا كان الجهاز مصابًا بهذه البرمجية، توصي اسيت بالتحقق من عدد من المؤشرات منها التحقق من وجود تطبيق باسم "ترقية جوجل" Google Update، ويتم ذلك من خلال اتباع المسار التالي: الضبط> مدير التطبيقات/ التطبيقات > "ترقية جوجل".

كما توصي الشركة بالتحقق من وجود تطبيق نشط لإدارة الجهاز تحت اسم "ترقية النظام" System update ويتم العثور عليه من خلال المسار : الضبط > الحماية> مسؤولو الأجهزة، بالإضافة إلى الظهور المتكرر لتنبيه "خدمة جوجل".

وفي حال وجود أي من المؤشرات آنفة الذكر، فمن المحتمل أن يكون جهاز المستخدم مصابًا بإحدى أشكال برمجية "بانكبوت". ولإزالة البرمجية الخبيثة يدويًا، يتعين على المستخدم القيام أولًا بتعطيل حقوق مديري الأجهزة الخاصة بتطبيق "ترقية النظام"، وبعدها إزالة تثبيت كل من "ترقية جوجل" وتطبيقات حصان طروادة المرتبطة به.

وعادة ما يعتبر العثور على تطبيق حصان طروادة التي تسبب بإصابة الجهاز بالبرمجية الخبيثة (وهو في هذه الحالة تطبيق "جويلز ستار كلاسيك") أمرًا معقدًا نظرًا لمهلة الـ 20 دقيقة التي تسبق نشاط البرمجية، إلى جانب عمل التطبيق على نحو اعتيادي لا يثير الشك ولتحديد وإزالة هذا التهديد من جميع مكونات الجهاز، فإننا ننصح باستخدام إحدى الحلول الأمنية الموثوقة والخاصة بالهواتف المحمولة

كيف يمكن الحفاظ على أمن الأجهزة؟

إلى جانب استخدام الحلول الأمنية الموثوقة والخاصة بالهواتف المحمولة، ثمة الكثير من الأمور الأخرى التي يتعين على المستخدم تجنبها حتى لا يصبح ضحية للبرمجيات الخبيثة الخاصة بالهواتف المحمولة والتي تشمل تفضيل متاجر التطبيقات المشروعة على المتاجر البديلة عندما يكون ذلك ممكنًا فإلى جانب كونه خاليًا من العيوب، يستعين متجر جوجل بلاي بتقنيات أمنية فائقة التطور قد لا تتوفر في المتاجر البديلة

وعند وجود شك حيال التطبيق الذي يتم تثبيته، يتعين على المستخدم التحقق من عدد التحميلات وتصنيفه والاطلاع على المحتوى الخاص بتقييماته و بعد تشغيل أي تطبيق على الهاتف المحمول، ينبغي للمستخدم الانتباه إلى الصلاحيات والحقوق التي يتطلبها ذلك التطبيق وفي حال مطالبة أي من التطبيقات بالحصول على أذونات تدخلية مشبوهة – ولا سيما الصلاحيات المتعلقة بالوصول – يتعين على المستخدم قراءتها بتمعن وعدم منحها الصلاحيات إلا بعد التأكد من موثوقيتها