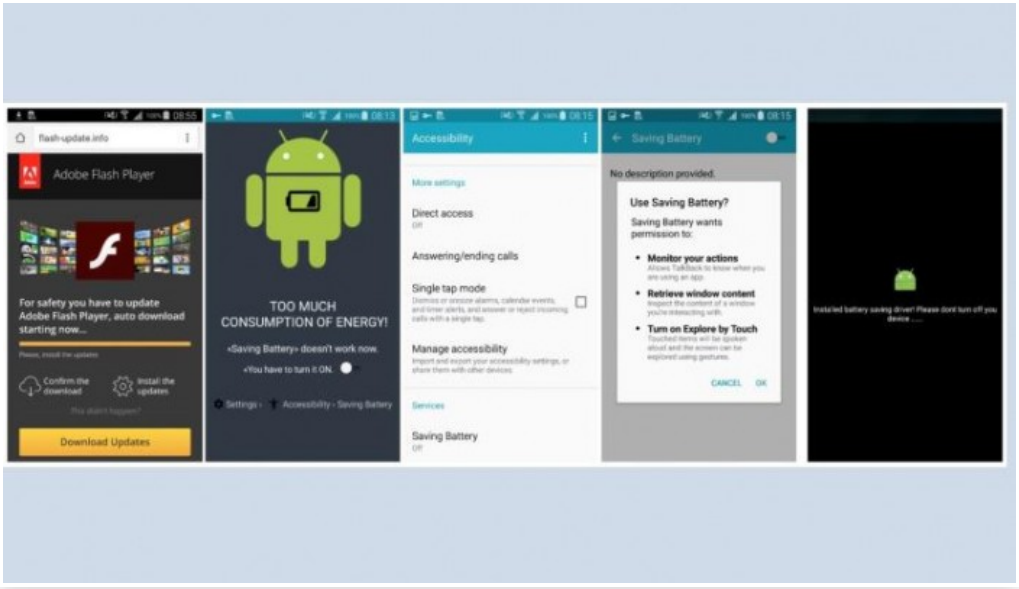
فيروس خطير يقلد نقرات المستخدم على أندرويد



الثلاثاء 21 فبراير 2017 07:02 م

كشفت شركة "إيسيت" (Eset) السلوفاكية لحلول الأمن الإلكتروني عن وجود تطبيق خبيث جديد من نوع حصان طروادة يقلد مشغل فلاش لشركة أدوبي ويعمل كنافذة وصول محتمل للعديد من الأنواع الخطيرة للبرمجيات الخبيثة.

واكتشف التطبيق تحت اسم (Android/Trojandownloader.Agent.JI) وهو يخدع ضحاياه لمنحه الأذونات الخاصة في قائمة الوصول ضمن أندرويد لاستخدامها في تنزيل وتنفيذ برمجيات خبيثة إضافية من اختيار المهاجمين.

وينتشر التطبيق عبر الموقع الإلكترونية المخترقة بما في ذلك مواقع التواصل الاجتماعي، ويستهدف الأجهزة العاملة بنظام أندرويد بما فيها الإصدارات الحديثة.

وأوضحت إيسيت أن بعض المواقع الإلكترونية تغري المستخدمين تحت ذريعة تدابير السلامة بتنزيل تحديث جديد وهمي لمشغل فلاش من أدوبي، وإذا وقع المستخدم في فخ نافذة التحديث وشغل عملية التثبيت فسيظهر له المزيد من النوافذ الوهمية.

وبعد استكمال عملية التثبيت بنجاح ستظهر النافذة المزيفة التالية رسالة تبلغ المستخدم باستهلاك هاتفه قدرا كبيرا من الطاقة، وتحثه على تشغيل نمط توفير طاقة البطارية مزيف.

وعلى غرار معظم النوافذ المنبثقة للبرمجيات الخبيثة لا تتوقف الرسالة عن الظهور حتى تنصاع الضحية للأمر فيتم الانتقال إلى قائمة إمكانيات الوصول في أندرويد التي تظهر مجموعة من الخدمات مع وظائف الوصول ومن بينها خدمة جديدة يشكلها البرنامج الخبيث خلال علمية التثبيت تحت اسم "توفير طاقة البطارية" والتي تطلب الإذن بمراقبة إجراءات المستخدم واسترداد محتوى النافذة وتفعيل الاستكشاف عبر اللمس، مما يتيح للمهاجم تقليد النقرات التي ينفذها المستخدم على شاشة الهاتف.

وبمجرد تمكين الخدمة تختفي أيقونة مشغل الفلاش الوهمية، إلا أن البرمجية الخبيثة تظل فعالة في الخلفية بالتواصل مع خادمها الخاص للقيادة والتحكم وتزوده بالمعلومات اللازمة عن الجهاز الضحية الذي يتحول إلى أداة بيد المهاجمين فيتمكنون من تنزيل وتركيب وتنفيذ وتنشيط حقوق مسؤول الجهاز دون الحاجة لموافقة المستخدم وبشكل غير مرئي تحت شاشة قفل وهمية.

وبعد استكمال الأنشطة السرية للتطبيق الخبيث تختفي شاشة القفل الوهمية ليعود المستخدم إلى استخدام جهازه لكن بعد أن يكون قد أصبح مخترقا.

وتوصي الشركة الذين يعتقدون أنهم ثبتوا هذا التحديث الوهمي لمشغل فلاش بإزالته يدويا من خلال مدير التطبيقات، وفي حال لم يتمكن المستخدم من حذفه بسبب حصول التطبيق على حقوق المسؤول عن الجهاز فإنه يمكن إلغاء تفعيل حقوق المسؤول من خلال التوجه إلى "الإعدادات" ثم "أمان" ثم "فلاش بلاير".

ونظرا لاحتمال أن يظل الجهاز مخترقا بعدد آخر من التطبيقات الخبيثة فإن الشركة توصي باستخدام أحد التطبيقات الأمنية حسنة السمعة للأجهزة المتنقلة.