تحذيرات من فيروس جديد لأجهزة "أندرويد" يسرق التفاصيل المصرفية!

دخل مستخدمو هواتف "أندرويد" في حالة تأهب قصوى بعد أن اكتشف الباحثون رسالة نصية جديدة خبيثة مصممة لسرقة التفاصيل المصرفية ومداهمة سجل العناوين الخاص بك.

فإذا تلقيت رسالة نصية من صديق أو جهة اتصال قريبة تطلب منك تنزيل تطبيق مشغل فيديو جديد، فكن حذراً.

ولتنفيذ هذا الهجوم المدمر، تستفيد الرسالة النصية من برنامج خبيث جديد، يُعرف باسم Flubot، يمكن أن يصيب أجهزة "أندرويد"، وبمجرد تثبيته، يكون لديه القدرات للسماح للمحتالين الإلكترونيين بسرقة بيانات الاعتماد المصرفية، واعتراض الرسائل النصية وحتى التقاط لقطات شاشة من جهاز الضحية.

و ما يزيد الطين بلة، يمكنه أيضا مداهمة سجل العناوين وتوزيع المزيد من الرسائل المزيفة على أي جهات اتصال يعثر عليها.

وفي الواقع، هذا هو أحد الأسباب التي تجعل خبراء الأمن قلقين للغاية بشأن Flubot، لأنه سيظهر دائما كما لو أرسلت الرسالة المزيفة من شخص تعرفه وتثق به.

ووفقا للخبراء في MalwareHunterTeam، عبر Computer Bleeping، يجب على مستخدمي "أندرويد" البحث عن أي رسائل نصية تسأل عما إذا كانوا يعتزمون تحميل مقطع فيديو من أجهزتهم.

وسيُضمّن رابط في الرسالة يأخذ الضحية لتزوير صفحة تنزيل لتطبيق Player Flash. وهذا التطبيق هو الذي سيبدأ كابوس Flubot، وإذا تلقيت رسالة تطلب منك تنزيل تطبيق خارج متجر "غوغل بلاي"، فإن النصيحة بسيطة: لا تفعل.

ويكمن أحد أسباب تأثر مستخدمي "أندرويد" دائما بهذه الحيل، في الطبيعة المفتوحة لنظام التشغيل هذا.

وعلى عكس آبل، التي تسمح فقط بتنزيل التطبيقات عبر متجر التطبيقات الرسمي الخاص بها، يمكن لمستخدمي "أندرويد" تثبيت الملفات والبرامج من أي مكان على الويب (بشرط أن يقوموا بتعديل الإعدادات الافتراضية لفتح الأشياء قليلا).

وهذا يعني أن المحتالين يمكنهم إنتاج تطبيقات مزيفة مليئة بالبرامج الضارة وتوزيعها مباشرة على الأجهزة التي تعمل بنظام "أندرويد"، دون الحاجة إلى التسلل تحت رادار ميزات أمان غوغل المضمنة في متجر "بلاي".

ولتجنب هجوم Flubot الأخير، يُنصح بعدم قيام مستخدمي "أندرويد" بالنقر فوق أي روابط خارجية غريبة حتى لو وضعت في نص من الأصدقاء.