5-اختراقات-أمنية-تجعل-الهواتف-الذكية-أكثر-عرضة-للخطر

مع وجود أخبار عن اختراق كبير كل أسبوع تقريبا هذا العام، قد يكون من الصعب معرفة ما إذا كانت بياناتك آمنة، حيث استهدف القراصنة الهواتف الذكية بتكرار متزايد، بهدف تتبع نشاط المستخدمين، أو سرقة بياناتهم أو خداعهم للكشف عن معلومات حساسة لتحقيق مكاسب مالية.

وعند التركيز بعض الشيء على الهجمات الإلكترونية الأخيرة، سنجد أن معظمها تستهدف أنظمة تشغيل الهواتف الذكية، ومتاجر التطبيقات. على سبيل المثال، اكتشف باحثون أمنيون في أيلول/سبتمبر وحده 172 تطبيقا ضارا على متجر غوغل بلاي، وقد حققت هذه التطبيقات أكثر من 335 مليون عملية تثبيت، كما لم تسلم شركات الاتصال من الاستهداف أيضا، حيث انتشرت عمليات الخداع المعروفة باسم SIM – والتي يحدث فيها تبديل رقم الهاتف إلى جهاز المتسلل – SIM splitting أو SIM swap، أو ما بات يعرف في الأوساط المختصة باسم مبادلة بطاقة ليتحكم بكل حساباتك المرتبطة به.

وبناء على ذلك، قد يكون أفضل حل لحماية بياناتك هو مراقبة جهازك عن كثب بحثا عن أي نشاط غير عادي، والاتصال بمزود الخدمة للتحقق من تعرض هاتفك الذكي للخطر.

فيما يلي أبرز 5 اختراقات أمنية حديثة تجعل الهواتف الذكية أكثر عرضة للخطر:

1- SimJacker: اختراق هاتفك برسالة نصية

الخاصة بالهواتف (SIM) في واحدة من أكبر الاختراقات التي حدثت خلال هذا العام، استخدم القراصنة ثغرة موجودة في معظم بطاقات الاتصال الذكية لتتبع مواقع المستخدمين، وفي بعض الحالات يمكنهم السيطرة الكاملة على أجهزتهم، وقد تأثر منه أكثر من مليار هاتف ذكي.

للأمن الإلكتروني في أيلول/سبتمبر الماضي. وكما يوحي الاسم، فإن AdaptiveMobile واكتشفته شركة SimJacker، عرف هذا الاختراق باسم الاختراق يجرى عن طريق رسالة نصية تحتوي على نوع معين من التعليمات البرمجية المشابهة لبرامج التجسس التي ترسل إلى هاتفك، وتعطي تعليمات لبطاقة الاتصال داخل الهاتف بالسيطرة على الجهاز لتنفيذ بعض الأوامر.

على نظام التشغيل، مما يعني أنه يمكن أن يؤثر على أي نوع من الأجهزة. ووفقا للتقارير، كانت معظم البلدان SimJacker لا يعتمد اختراق المتأثرة في الشرق الأوسط، وإفريقيا.

هجمات التصيد بالرسائل القصيرة لهواتف أندرويد -2

والذي استهدف بعض الهواتف الحديثة التي ،(SMS) هجوم تصيد عبر الرسائل القصيرة Check Point اكتشف الباحثون في شركة الأمن الإلكتروني وذلك من خلال رسائل تهدف إلى خداع المستخدمين لتغيير إعدادات الهواتف ومنح المتسللين حق ،Android (تعمل بنظام التشغيل (أندرويد .الوصول إلى معلوماتهم

ومن أبرز الهواتف التي تعرضت لهذا الهجوم، كانت هواتف أكبر الشركات في السوق ومنها سامسونغ، وهواوي، وإل جي، وسوني. وقد أرسل المتسللون رسائل للمستخدمين مشابهة لرسائل مشغل الشبكة، يطلبون منهم تنزيل تطبيق على الهاتف لضبط الإعدادات الخاصة بالشبكة على هاتف جديد. وفي حالة الموافقة على التنزيل، سيقوم جهازك بإعادة توجيه بياناته عبر خادم المتسللين، مما يتيح لهم الوصول إلى رسائل .البريد الإلكتروني وقوائم جهات الاتصال، ونشاط المتصفح

وهواوي بالفعل بتصحيح لهذه الثغرة الأمنية خلال أيلول/سبتمبر الماضي، ولا تعتقد شركة سوني أن ،LG كذلك قامت كل من سامسونغ، و .Checkpoint أجهزتها معرضة للخطر، وفقا لتقرير شركة

وإذا كنت غير متأكد من حصول هاتفك على تحديث نظام التشغيل الذي يتضمن التصحيح، فيجب عليك رفض تنزيل أي تطبيق من رقم غير .معروف، واتصل بمزود الخدمة مباشرة إذا تلقيت رسائل مشبوهة

الاختراق عبر مقاطع فيديو -3

في وقت سابق من صيف هذا العام، أدركت أجهزة مراقبة الأمن الإلكتروني أن هواتف أندرويد كانت عرضة للاختراق بمجرد مشاهدة مقاطع .فيديو بها برامج ضارة مدمجة

المشكلة ونشر إثباتا للمفهوم يوضح كيف يمكن لمستخدمي نظام التشغيل أندرويد أن يتعرضوا للاختراق Marcin Kozlowski وحدد الباحث الأمني إذا قاموا بتنزيل ملف فيديو ضار وتشغيله على أجهزتهم، حيث يسمح ذلك للمهاجم عن بعد بتنفيذ تعليمات برمجية عشوائية على الجهاز .المستهدف

كما أصدرت غوغل تصحيحا للثغرة الأمنية في تموز/يوليو الماضي. إذا لم تكن قد قمت بتنزيل ملف فيديو على هاتف أندرويد الخاص بك، فمن المحتمل أن هاتفك لم يتضرر - لأن مقاطع الفيديو التي يتم تشغيلها من خلال تطبيقات الطرف الثالث مثل واتساب، ومسنجر ليست عرضة .للبرامج الضارة - لكن يجب عليك التأكد من تحديث نظام التشغيل أندرويد بالكامل لضمان حماية هاتفك

iOS عدة ثغرات أمنية في نظام التشغيل -4

التابع لشركة (iOS) ست نقاط ضعف في نظام التشغيل آي أو إس (Project Zero) اكتشف اثنان من الباحثين في فريق البحث عن الأخطاء في غوغل .(iOS 12.4) آبل خلال تموز/يوليو الماضي، وقد صححت آبل خمس نقاط ضعف عبر تحديث نظام التشغيل

ثغرة أمنية أخرى في مجموعة من المواقع الإلكترونية المخترقة خلال آب/أغسطس، والتي تسببت في اختراق (Project Zero) واكتشف فريق .هواتف آيفون على مدار سنوات

كما لم يكشف عن عدد محدد للمستخدمين المتأثرين، حيث تعمل البرامج الضارة في خلفية الأجهزة دون أي وسيلة لاكتشافها. ولم تحدد .غوغل مواقع الويب التي يمكن أن تصيب هواتف المستخدمين

إذا لم تكن متأكدا مما إذا كان هاتف آيفون iOS 12.1.4. ومع ذلك، بمجرد إخطار آبل بالثغرة قامت بتضمين تصحيح أمان في إصدار نظام التشغيل .أو إصدار أحدث iOS 12.1.4 الخاص بك قد تأثر، فإن الخيار الأكثر أمانا هو التأكد من أنك تعمل على نظام التشغيل

5- استغلال واتساب لاختراق هواتف آيفون وأندرويد

خلال أيار/مايو الماضي؛ كشف تقرير لصحفية فاينانشال تايمز أن مجموعة من القراصنة قاموا باستغلال تطبيق التراسل واتساب لتثبيت برامج تجسس عن بعد على هواتف المستخدمين سواء التي تعمل على نظام التشغيل أندرويد، أو آي أو إس، وذلك عن طريق الإجابة على .مكالمات صوتية لجهات اتصال غريبة

وبمجرد اكتشاف شركة واتساب للثغرة، أجرت التغييرات المطلوبة على بنيتها التحتية لتصحيحها. كذلك حثت مستخدمي التطبيق على الترقية إلى أحدث إصدار، بالإضافة إلى تحديث نظام تشغيل الهاتف، بهدف الحماية من الاختراقات المحتملة، ومنع وصول القراصنة إلى .المعلومات المخزنة على الأجهزة المحمولة