جوزيف كوكس | نشر في ١٧ نوفمبر ٢٠٢٠,

كيف يشتري الجيش الأمريكي بيانات تحديد المواقع من تطبيقات الهاتف؟

ترجمة وتحرير نون بوست

علمت مجموعة "ماذربورد" أن الجيش الأمريكي يشتري بيانات تنقل للأشخاص حول العالم، يتم جمعها من تطبيقات تبدو غير ضارة. من بين تلك التطبيقات التي اكتشفت ماذربورد أن لها علاقة بعمليات جمع بيانات المستخدمين، مثل تطبيق أوقات صلاة للمسلمين الذي تم تنزيله أكثر من 98 مليون حول العالم. ومن بينها أيضا تطبيق مواعدة إسلامي، وتطبيق "كريغليست الشهير، وتطبيق توقعات لحالة الطقس، وتطبيق "ليفل" الذي يمكن استخدامه للمساعدة في تثبيت الرفوف في غرفة النوم.

من خلال سجلات ومقابلات مع مطورين وعمليات تحليل فني، كشفت مجموعة ماذربورد عن تدفقات للبيانات يستخدمهما الجيش الأمريكي، أو تم استخدامها في السابق، للحصول على معلومات عن مواقع الأشخاص.

ويأتي الجزء الأول من البيانات من شركة "بابل ستريت"، التي توفر منتجًا يُعرف بـ"لوكيت إكس"، تستخدمه قيادة العمليات الخاصة للجيش الأمريكي، وهو الفرع المكلف بمكافحة الإرهاب والتمرد ومهام الاستطلاع الخاصة. وقامت قيادة العمليات الخاصة بشراء بيانات "لوكيت أكس" لتسهيل مهام قواتها في المهام الخارجية. بينما يأتي الجزء الثاني من شركة "إكس مود"، والتي تحصل على بيانات مباشرة من التطبيقات، ثم تبيع تلك البيانات للوكلاء ومن ثم إلى الجيش الأمريكي.

بدأت الأضواء تُسلط مؤخرا على بيع بيانات تحديد المواقع بطرق غير شفافة، وحقيقة أن الجيش الأمريكي متورط في الحصول على معلومات حساسة، وقد استخدم بيانات أخرى لتحديد أهداف والقيام بهجمات بالطائرات المسيرة.

ويعد المسلمون من بين مستخدمي هذه التطبيقات التي تُأخذ منها البيانات، وهو أمر جدير بالملاحظة

بالنظر إلى أن الولايات المتحدة قد شنت حروبًا استمرت عقودًا على الجماعات الإرهابية ذات الأغلبية المسلمة في الشرق الأوسط، وقتلت مئات الآلاف من المدنيين خلال العمليات العسكرية التي شنتها في باكستان وأفغانستان والعراق. ولم تحصل مجموعة ماذربورد على معلومات محددة حول العمليات القتالية التي استخدم فيها الجيش الأمريكي هذا النوع من بيانات تحديد المواقع المأخوذة من التطبيقات.

من بين التطبيقات التي تُرسل البيانات إلى "إكس مود" تطبيق "مسلم برو"، وهو تطبيق يذكّر المستخدمين بمواعيد الصلاة ويحدد اتجاه القبلة. وفقا لمتجر غوغل بلاي، تم تنزيل التطبيق أكثر من 50 مليون مرة على أندرويد. وفي المجموع، تم تنزيله أكثر من 98 مليون مرة عبر المنصات المختلفة، بما في ذلك الأجهزة التي تعمل بنظام آي أو إس، وفقًا لموقع مسلم برو الإلكتروني.

يُعرّف "مسلم برو" نفسه على الموقع الإلكتروني بأنه التطبيق الإسلامي الأكثر انتشارا، وهو يتضمن مقاطع وتلاوات صوتية للقرآن. كما يُرسل "مسلم منغل"، وهو تطبيق مواعدة تم تنزيله أكثر من 100 ألف مرة، بياناته إلى شركة "إكس مود".

لم يكن بعض مطوري التطبيقات التي تحدثت إليهم مجموعة ماذربورد على دراية بالجهات التي تصل إليها بيانات مواقع مستخدميهم. وحتى إذا قام المستخدم بتعديل سياسة خصوصية التطبيق، فمن المحتمل ألا يدرك في نهاية المطاف عدد الشركات أو الوكالات الحكومية التي تشتري بياناته.

أثار شراء قوات إنفاذ القانون الأمريكية هذه المعلومات تساؤلات حول شرعية حصول السلطات على بيانات تحديد المواقع التي قد تتطلب عادةً إذنا للوصول إليها. لكن العقد الذي أبرمته قيادة العمليات، وبعض التقارير الأخرى، تقدم أكبر دليل على أن هذه البيانات لا تصل إلى قوات إنفاذ القانون فحسب، بل تصبح متاحة للجيش الأمريكي.

وفقًا لسجلات المشتريات التي حصلت عنها مجموعة ماذربورد، اشترت قيادة العمليات الخاصة حق الوصول إلى بيانات تحديد المواقع من برنامج "لوكيت أكس"، التابع لشركة "بابل ستريت". وقد شرح موظف سابق في "بابل ستريت" لـ"ماذربورد" كيف يمكن لمستخدمي المنتج مراقبة الأجهزة التي تحتوي على بيانات تملكها الشركة عبر التطبيقات المختلفة، وبالتالي تتبع تنقلات المستخدمين وتحديد مواقعهم بدقة.

لا تُحدّد بيانات "لوكيت إكس" هوية المستخدمين، لكن الموظف السابق أكد أن الشركة يمكنها أن تكشف عن هوية أي شخص، وأن موظفيها يمكنهم استغلال تلك البيانات.

وفقا للسجلات، اشترت قيادة العمليات الخاصة بالجيش الأمريكي في نيسان/ أبريل الماضي "تراخيص برامج إضافية" من لوكيت إكس، ومنتجا آخر يساعد على تحليل النص يسمى "بابل إكس". تُظهر السجلات أن التراخيص الإضافية كلفتها حوالي 90 ألف دولار.

في بيان، أكد تيم هوكينز، المتحدث باسم قيادة العمليات الخاصة الأمريكية، شراء بيانات لوكيت إكس، وأضاف: "نستخدم هذا البرنامج لدعم مهام قوات العمليات الخاصة في الخارج. نحن نلتزم بشدة بالإجراءات والسياسات المعمول بها لحماية الخصوصية والحريات المدنية، ناهيك عن الحقوق الدستورية والقانونية للمواطنين الأمريكيين".

حسب وثيقة من بابل ستريت متاحة عبر الإنترنت، فإنه "من بين الخصائص الفنية لبيانات لوكيت أكس، أن استخدام العميل للبيانات ليس محدّدا بعدد عمليات البحث". وجاء في الوثيقة ذاتها أن "بيانات الموقع قد لا تكون دقيقة دائمًا". لم تستجب شركة بابل ستريت لطلبات التعليق المتعددة التي أُرسلت إليها.

خلال شهر آذار/ مارس، أفاد منشور بروتوكول التكنولوجيا لأول مرة أن وكالات إنفاذ القانون الأمريكية، مثل هيئة الجمارك وحماية الحدود ووكالة إنفاذ قوانين الهجرة والجمارك بالولايات المتحدة، كانت تستخدم بيانات لوكيت أكس. في هذا السياق، حصلت مجموعة ماذربورد على وثيقة سرية تؤكد استخدام الوكالة لهذه البيانات. اشترت بعض الوكالات الحكومية، بما في ذلك هيئة الجمارك وحماية الحدود ودائرة الإيرادات الداخلية بيانات تحديد المواقع من شركة أخرى تُعرف باسم "فينتل".

في هذا الإطار، قال مارك تالمان، الأستاذ المساعد في قسم إدارة الطوارئ والأمن الداخلي في أكاديمية ماساتشوستس البحرية، في رسالة بالبريد الإلكتروني لمجموعة ماذربورد: "من وجهة نظري، من المؤكد عمليًا أن الكيانات الأجنبية ستحاول الاستفادة (أو هي تقوم بذلك فعلا) من مثل هذه المصادر التي توفر بيانات خاصة بالمستخدمين. وأعتقد أنه سيكون من السذاجة افتراض عكس ذلك".

سلسلة التوريد

تحصل بعض الشركات على بيانات تحديد المواقع من التطبيقات عبر ما يُعرف بـ"بيانات تدفق عروض الأسعار"، وهي معلومات يتم جمعها من المزادات في "الوقت الفعلي" عندما يدفع الناشرون مقابل إظهار إعلاناتهم للمتصفحين. غالبا ما تحصل الشركات أيضا على البيانات من حزمة أدوات تطوير البرمجيات.

تشجع بيانات "إكس مود"، والتي تختلف عن "بابل ستريت"، مطوري التطبيقات على دمج حزمة أدوات تطوير البرمجيات، وهي عبارة عن حزمة من التعليمات البرمجية، في تطبيقاتهم الخاصة. تجمع حزمة أدوات تطوير البرمجيات بعد ذلك بيانات مواقع مستخدمي التطبيق وترسلها إلى "إكس مود". في المقابل، تدفع الشركة لمطوري التطبيق رسوما بناء على عدد المستخدمين. على سبيل المثال، قد يجني المطور 1500 دولار شهريا من تطبيق يضم 50 ألف مستخدم نشط يوميا في الولايات المتحدة، وذلك وفقا لموقع "إكس مود" الإلكتروني.

في مقابلة حديثة مع شبكة سي إن إن، قال الرئيس التنفيذي لشركة "إكس مود"، جوشوا أنتون، إن الشركة تتعقب 25 مليون جهاز داخل الولايات المتحدة كل شهر، و40 مليون جهاز في أماكن أخرى، بما في ذلك في الاتحاد الأوروبي وأمريكا اللاتينية ومنطقة آسيا والمحيط الهادئ. وأكدت شركة "إكس مود" لمجموعة ماذربورد سابقا أن حزمة أدوات تطوير البرمجيات الخاصة بها موجودة في حوالي 400 تطبيق.

في تشرين الأول/ أكتوبر، نشرت لجنة المنافسة وحماية المستهلك الأسترالية تقريرا حول عمليات نقل البيانات بواسطة تطبيقات الهواتف الذكية. كشف قسم من هذا التقرير عن "نقطة النهاية" – وهي عنوان محدد موقع الموارد المُوحّد الذي تستخدمه بعض التطبيقات – لإرسال بيانات تحديد المواقع مرة أخرى إلى "إكس مود". كما قام مطورو تطبيق "ذي غارديان"، المصمم لحماية المستخدمين من سرقة بيانات مواقعهم، بنشر "نقطة النهاية". بعد ذلك، استخدمت مجموعة ماذربورد نقطة النهاية هذه لاكتشاف التطبيقات التي ترسل بياناتها إلى "الوسيط".

استخدمت مجموعة ماذربورد برنامجا لتحليل الشبكات لمراقبة تطبيق "مسلم برو" بنسختي أندرويد و"آي أو إس"، وهو يرسل بيانات تحديد المواقع إلى "نقطة نهاية" في "إكس مود" عدة مرات.

في هذا الصدد، يقول ويل ستارفاش، المتخصص في نظام آي أو إس ومؤسس تطبيق "ذي غارديان"، إنه لاحظ أيضا أن نسخة آي أو إس من تطبيق "مسلم برو" ترسل بيانات تحديد مواقع المستخدمين إلى "إكس مود".

ووفقا لما حصلت عليه ماذربورد من معلومات، تضمّن نقل البيانات اسم شبكة الواي فاي التي يتصل بها الهاتف، والختم الزمني، ومعلومات حول الهاتف نفسه، مثل طرازه. ولم يستجب تطبيق "مسلم

برو" لطلبات التعليق المتعددة.

من بين التطبيقات الأخرى التي ترسل البيانات إلى "إكس مود" تطبيق عداد الخطوات "أكوبيدو"، والذي تم تنزيله أكثر من خمسة ملايين مرة وفقا لصفحة التطبيق على متجر غوغل بلاي. هناك أيضا تطبيق "سي بلس فور كريغسليست" الذي يتيح للمستخدمين البحث في موقع كريغسليست بسهولة أكبر، وقد تم تنزيله أكثر من مليون مرة، و"غلوبل ستورمز"، وهو تطبيق لمتابعة الأعاصير والعواصف الاستوائية، وتم تنزيله أكثر من مليون مرة.

بالإضافة إلى تطبيق "مسلم برو"، قامت مجموعة ماذربورد أيضا بتثبيت تطبيق "مسلم منغل" للتعارف على هاتف أندرويد ولاحظت أن التطبيق يرسل إحداثيات دقيقة للموقع الجغرافي لمكان الهاتف في تلك اللحظة واسم شبكة الواي فاي إلى "إكس مود" عدة مرات. ولم تستجب شركة "منغل" المالكة للتطبيق ومقرها في فيتنام، لطلبات التعليق المتعددة.

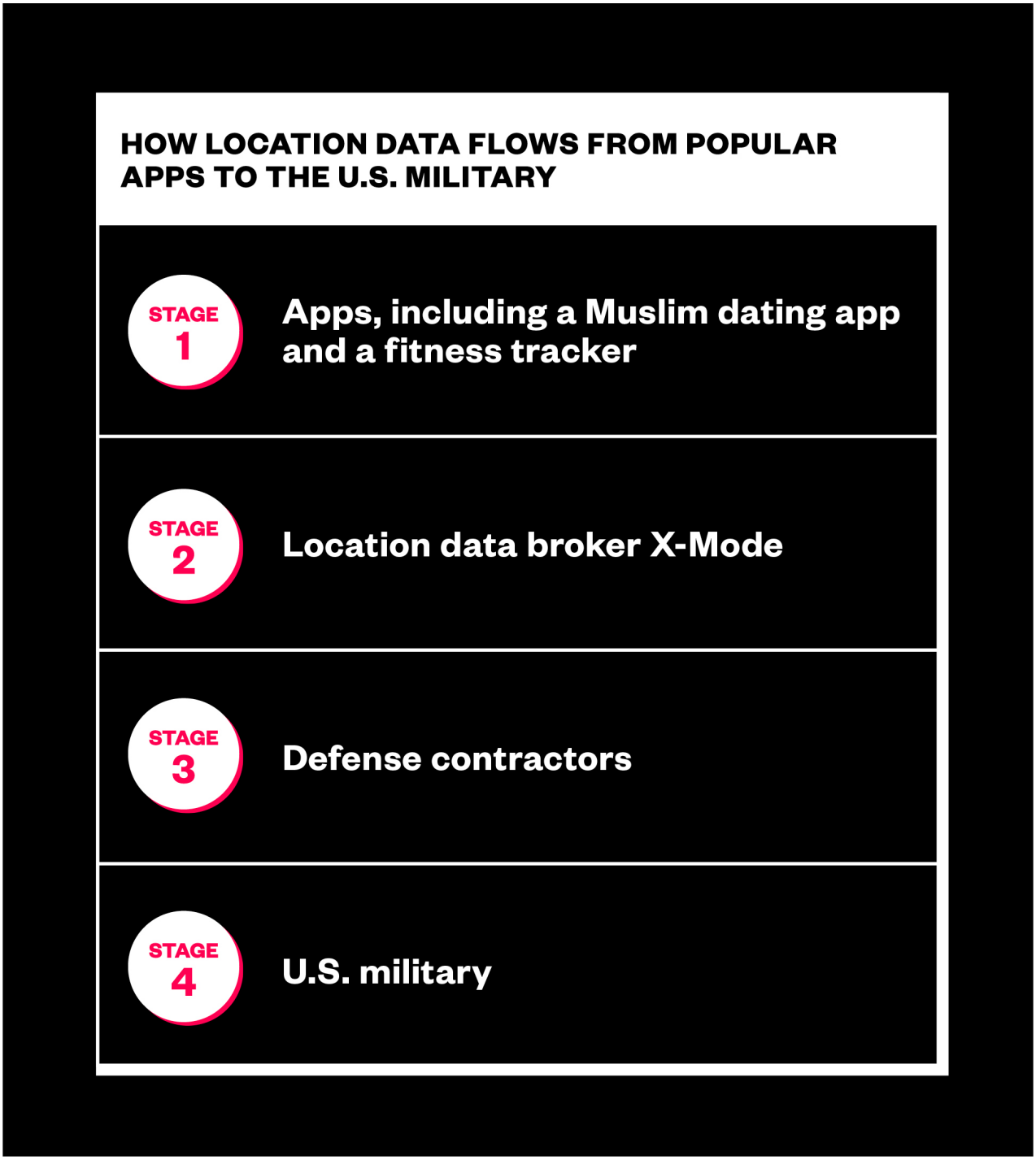
وقد رصدت مجموعة ماذربورد شبكة أخرى من تطبيقات المواعدة التي تعمل بشكل متطابق تقريبا مع "منغل"، وتقوم بإرسال بيانات تحديد المواقع إلى "إكس مود".

قامت مجموعة ماذربورد بتنزيل تطبيق مواعدة آخر يسمى "إيران سوشل"، على جهاز اختبار ولاحظت عملية إرسال إحداثيات نظام التموضع العالمي إلى "إكس مود". تشمل هذه الشبكة أيضا "تركي سوشل" و"إيجبت سوشل" و"كولومبيا سوشل"، وغيرها من التطبيقات التي تركز على بلدان معينة.

بعد ذلك، تقوم شركة "إكس مود" ببيع حق استخدام هذا النوع من البيانات لمجموعة واسعة من العملاء. كشفت مجموعة ماذربورد في وقت سابق أن أحد هؤلاء العملاء هو شركة استخبارات خاصة هدفها استخدام بيانات تحديد المواقع لتعقب الأشخاص وصولا إلى منازلهم. كما كشفت شركة "إكس مود" أيضا كيف يمكن استخدام بياناتها لمتابعة الأماكن التي ذهب إليها الأشخاص الأكثر عرضة للإصابة بكوفيد19.

وجدت مجموعة ماذربورد أن من بين عملاء "إكس مود"، متعاقدون تابعون للجيش الأمريكي. أدرجت "إكس مود" شركتي "سييرا نيفادا كوربوريشن" و"سيستمز أند تكنولوجي ريسرتش" ضمن قائمة "الشركاء الموثوق بهم" وفق موقعها على شبكة الإنترنت.

تصنع شركة "سييرا نيفادا كوربوريشن" طائرات مقاتلة للقوات الجوية الأمريكية، وتدعم شركة "نورثروب غرومان" في تطوير قدرات الجيش الأمريكي على شن الحروب الإلكترونية و السيبرانية. من جهتها، تعمل شركة "سيستمز أند تكنولوجي ريسرتش" مع القوات البرية والبحرية والجوية وفقا لسجلات المشتريات، وتقدم الدعم في مجال "تحليل البيانات" لمحللي الاستخبارات، وفقا لموقعها على الإنترنت.



وقد أكد السيناتور رون وايدن لمجموعة ماذربورد في بيان أن شركة "إكس مود" صرحت أنها تبيع بيانات تحديد المواقع التي تجمعها من هواتف الأمريكيين لعملاء في الجيش الأمريكي. وجاء في البيان: "خلال مكالمة مع مكتبي في أيلول/ سبتمبر، أكد محامو وسيط البيانات إكس مود سوشل أن الشركة تبيع البيانات التي يتم جمعها من الهواتف في الولايات المتحدة إلى عملاء من الجيش الأمريكي، عبر مقاولين. وبحجة اتفاقيات الحفاظ على السرية، رفضت الشركة تحديد المقاولين أو الوكالات الحكومية التي تشتري البيانات".

من جهة أخرى، أكدت "إكس مود" لمجموعة ماذربورد في رسالة بالبريد الإلكتروني أنها "لا تعمل مع سييرا نيفادا كوربوريشن أو سيستمز أند تكنولوجي ريسرتش"، لكنها لم تنكر أن الشركتين كانتا من

عملائها في السابق. (مع استمرار مجموعة ماذربورد في التقصي عن نشاط الشركة، ومواصلة مكتب السيناتور رون وايدن تحقيقاته بشأن بيع بيانات تحديد المواقع، أزالت شركة "إكس مود" أسماء شركات متعددة من صفحة "الشركاء الموثوق بهم" على موقعها الإلكتروني، بما في ذلك شركة سيبرا نيفادا كوربوريشن).

أضافت شركة "إكس مود" في بريدها الإلكتروني أنها "تتيح لوحة البيانات لعدد صغير من شركات التكنولوجيا التي قد تعمل مع الوكالات العسكرية الحكومية، لكن عملنا مع هؤلاء المتعاقدين له طابع دولي ويركز بشكل أساسي على ثلاث حالات استخدام: مكافحة الإرهاب والأمن السيبراني والتنبؤ ببؤر انتشار فيروس كوفيد19 في المستقبل".

أخبرنا العديد من مطوري التطبيقات الذين يعملون مع "إكس مود" أنهم لا يعرفون أنه تم إرسال بيانات مواقع مستخدميهم إلى مقاولين يعملون مع الجيش الأمريكي.

كتب نيكولا دودوش، الرئيس التنفيذي لشركة تطوير التطبيقات "موب زاب"، في رسالة بالبريد الإلكتروني إلى ماذربورد: "لم أكن على علم بأن "إكس مود" كانت تبيع هذه البيانات لبعض المتعاقدين العسكريين".

وكانت شركة "موب زاب" قد أنشأت تطبيقًا لمشاركة الشاشة يعمل بنظام أندرويد، ويرسل بيانات تحديد المواقع إلى إكس مود، وتم تنزيل التطبيق أكثر من مليون مرة. وأضاف دودوش: "لم أكن لأعلم أن إكس مود يعمل مع متعاقدين عسكريين لأنهم لم يذكروا ذلك بشكل صريح".

من جهته، قال أنطوان فياني، مطور تطبيق "بابل ليفل" الذي بلغ عدد مرات تنزيله حوالي عشرة مليون مرة: "بصفتي مطور تطبيقات، فأنا أهتم بمن أتعاقد معه". لكنه يستدرك قائلا: "لأكون واضحا تماما، لا أتذكر الشركتين اللتين أرسلتهما لي"، في إشارة إلى شركتي "سيبرا نيفادا كوربوريشن" و"سيستمز أند تكنولوجي ريسرتش".

كما يبدو أن شركة يان فليكس التي قامت بتطوير تطبيق "سي بلس فور كريغسليست" لم تكن على علم أيضا بأن "إكس مود" تعمل مع مقاولين عسكريين. أرسلت يان فليكس ردا بالبريد الإلكتروني جاء فيه: "لا أعتقد أن ما وصفته صحيح".

من جانبه، أكد تطبيق تتبع الخطوات "أكوبيدو"، لماذربورد في رسالة بالبريد الإلكتروني: "نحن لا نتحدث علنًا عن العلاقات التي تربطنا مع شركائنا. إن كنت مهتمًا بعلاقتنا مع "إكس مود"، يمكنك التواصل معهم مباشرة".

وقال نيل كيلي، رئيس شركة "كيلي تكنولوجي"، التي عملت على تطوير تطبيق "غلوبل ستورمز"، في رسالة بالبريد الإلكتروني: "نحن نشعر بالاطمئنان حيال استخدام إكس مود لبيانات تحديد المواقع".

في موقعها على الإنترنت، تتحدث "إكس مود" عن "أفضل الممارسات" التي يتم من خلالها الحصول على موافقة مستخدمي التطبيقات لجمع بيانات مواقعهم. وبالإضافة إلى الإذن المسبق ضمن نظام التشغيل للوصول إلى تلك البيانات، وسياسة الخصوصية، تقول إكس مود إنها قادرة على "تزويد الشركاء باللغة المناسبة لتيسير عملية التصفح الآمن، ولتحقيق التوافق مع الطريقة التي نعرض بها البيانات التي نجمعها ونقدمها لمستخدمي منصاتنا".

تجدر الإشارة بأن نافذة بنود خدمة تطبيق "بابل ليفل" التي تظهر عندما يفتح المستخدم التطبيق لأول مرة، تشير إلى أن البرنامج قد يجمع بيانات تحديد المواقع "لتشغيل إعلانات موجهة وتحليلات مكانية وصلاحيات وغيرها من الأبحاث المدنية والاستهلاكية والعلمية بخصوص حركة المرور والأماكن المكتظة".

ويقدم تطبيق "غلوبل ستورمز" نصا مشابها حسب اختبارات ماذربورد. ولا تشير بنود إخلاء المسؤولية بصراحة إلى أنه سيتم إرسال البيانات إلى مقاولين عسكريين أو شركات استخبارات خاصة. بل وتنص بنود سياسة الخصوصية لبعض التطبيقات، كما هو الحال في "إكس مود"، على أن الشركة قد تستخدم بيانات تحديد المواقع "لأبحاث الأمراض والوقاية منها، والأمن، ومكافحة الجريمة، وتطبيق القانون".

وقال كيلي عن مستخدمي تطبيق "غلوبل ستورمز": "لست على علم بعدد الذين يقدمون الموافقة".

لكن بعض التطبيقات التي تجمع بيانات تحديد المواقع نيابة عن إكس مود تقوم بإخفاء عملية نقل البيانات. حيث لا تتطرق بنود سياسة الخصوصية في تطبيق "مسلم برو" إلى ذكر شركة "إكس مود"، ولا يقدم التطبيق عند تثبيت أو فتح التطبيق أي نوع من المعلومات التي قد توضّح للمستخدم عملية نقل بيانات تحديد المواقع. إلا أن سياسة خصوصية "مسلم برو" تنص على أن التطبيق يعمل مع شركتي "توتيلا" و"كوادرنت"، وهما شركتان متخصصتان في بيانات تحديد المواقع. وقد تتبعت ماذربورد نقلا للبيانات إلى "توتيلا".

لم يقدم تطبيق "مسلم منغل" أي نافذة لإخلاء المسؤولية في اختبارات ماذربورد كذلك، ولم تتطرق بنود سياسة خصوصية التطبيق إلى شركة "إكس مود" على الإطلاق. وينضم إليه تطبيق "إيران سوشل"، أحد التطبيقات في الشبكة الثانية لتطبيقات المواعدة التي تتشارك بكود برمجة واحد في الأغلب، حيث يفتقر أيضًا لأي معلومات حول بيع بيانات تحديد المواقع.

عقب اختبارات ماذربورد، والتواصل مع التطبيقين للتعليق، أضاف "مسلم منغل" نافذة جديدة تصرح بأن التطبيق يجمع بيانات تحديد المواقع. وقامت شركة "إنوفيت ديتنغ"، المسؤولة عن "إيران سوشل"، بالمثل.

أوضحت "إكس مود" في رسالة بالبريد الإلكتروني إلى ماذربورد أن التطبيقات الشريكة لها ملزمة تعاقديًا باتباع قوانين حماية البيانات ذات الصلة والحصول على الموافقة، بدلاً من وضع آلية فنية توقف تجميع البيانات إن لم يتم الحصول على موافقة صريحة.

وجاء في رسالتها: "نحن نطلب من جميع التطبيقات الموجودة على منصتنا اتباع جميع قوانين الخصوصية وحماية البيانات المعمول بها وإرشادات نظم التشغيل المسؤولة (كنظام أندرويد لغوغل، ونظام أو إس لأبل). شركاؤنا من التطبيقات ملزمون تعاقديًا بالامتثال لهذه المتطلبات. وتشمل تلك المتطلبات الحصول على كل ما هو مطلوب من الموافقات والأذونات من المستخدمين النهائيين لأي عملية جمع واستخدام للبيانات".

وأضافت: "نوفر لشركائنا من التطبيقات أدوات لإدارة الموافقات لمساعدتهم على الامتثال لهذه المتطلبات، ونقوم بتدقيق تطبيقات الناشرين للتأكد من توافقها. وعندما نجد أي مشكلة تشير لعدم التزام أحد التطبيقات على منصتنا، فإننا نأخذ ذلك على محمل الجد، ونتحقق بدقة ثم نتخذ الإجراءات المناسبة".

عندما عُرض على كريس هوفناغل أمثلة لبعض بنود سياسة الخصوصية الضعيفة لدى التطبيقات، أرسل مدير هيئة التدريس في مركز بيركلي للقانون والتكنولوجيا بريدا إلكترونيا لمجموعة ماذربورد، قال فيه إن "السؤال الذي يجب طرحه هو ما إذا كان المستهلك العاقل لهذه الخدمات سيتنبأ بهذه الاستخدامات ويوافق عليها، إن طُلب منه ذلك بنص صريح. فمن السليم القول في هذا السياق، إن المستخدم العاقل العقلاني – الذي لا يعد خبيرًا في مجال التكنولوجيا – لن يتصور أن بياناته سُتستخدم على نطاق عسكري، حتى لو قرأ ما تم الإفصاح عنه".

كانت شركة سيبرا نيفادا مسؤولة عن تقرير تم التشكيك في مصداقيته على نطاق واسع، حيث استخدم

ذلك التقرير بيانات تحديد المواقع لاستنتاج وقوع حدث تخريبي في معهد ووهان لأبحاث الفيروسات في تشرين الأول/ أكتوبر 2019.

حتى الآن، لم تستجب شركتا "سييرا نيفادا كوربوريشن" و"سيستمز أند تكنولوجي ريسرتش" لطلباتنا المتعددة للتعليق.

المصدر: فايس

رابط المقال: https://www.noonpost.com/38930/