العرب
الأحد 2020/02/02
السنة 42 العدد 11605

أفاست.. برنامج مضاد للفيروسات وجاسوس

شركات تدفع للبرنامج من أجل الاطلاع على بيانات المستخدمين كاملة

لم تعد برامج مكافحة الفيروسات المجانية "مجانية" بحق وآمنة، ذلك ما بينه الخبير التكنولوجي كريس هوفمان حيث كشف أن برنامج مكافحة الفيروسات "أفاست" يقوم بجمع بيانات تصفح المستخدمين لبيعها إلى أطراف ثالثة، وهو ما أكده تحقيق مشترك تعاون على إنجازه موقعا "بي. سي ماغ" و"ماذر بورد" المختصان في التكنولوجيا.

واشنطن - تحولت بيانات المستخدمين إلى مصدر إثراء لشركات التكنولوجيا، غير أن هذه المعطيات غير محصنة من التجسس والبيع لفائدة شركات عالمية تحلل سلوك الزبائن باستخدام هذه البيانات، مما يمنحها قوة هائلة في سوق الإعلانات.

وفي الآونة الأخيرة كشف تحقيق مشترك تعاون على إنجازه موقعا "بي. سي ماغ" و"ماذر بورد" المختصان في التكنولوجيا عن تورط برنامج أفاست المضاد للفيروسات، في جمع بيانات تصفح المستخدمين لبيعها إلى أطراف ثالثة، ويعدّ هذا أحدث مثال على ما تقترفه البرامج المجانية من استخدام غير مشروع للمعطيات والبيانات الشخصية.

كريس هوفمان

برنامج أفاست المضاد للفيروسات يجمع بيانات تصفح المستخدمين لبيعها إلى أطراف ثالثة

وكشف كريس هوفمان، مدير تحرير موقع "هاو - تو جك" المتخصص في البرامج التكنولوجية، في تقرير أعده حول برنامج مكافحة الفيروسات أفاست المضاد للفيروسات، أنه يجمع بيانات تصفح المستخدمين لبيعها إلى أطراف ثالثة، وهو ما أكده تحقيق مشترك تعاون عليه موقعا "بي.سي ماغ" و"ماذربورد" المختصان في التكنولوجيا. وهو دليل جديد على تورط برنامج مجاني لمكافحة الفيروسات في جمع البيانات. ويعتبر البعض في هذا الاكتشاف دليلا على تطور منطقي للأحداث، حيث يحتاج مبرمجو هذه الخدمات المجانية إلى كسب المال بطريقة أو بأخرى.

وشهدت في السنوات الأخيرة مسألة بيع المعطيات الشخصية ازدهارا مطّردا، حيث تقوم العديد من الشركات المتخصصة، وشركات الاتصالات والمطاعم والمستشفيات والجامعات والمحلات التجارية وحتى صالونات الحلاقة.. بجمع كميات كبيرة من البيانات حول زبائنها وبيعها.

وبالنسبة للشركات الكبرى فإن هذا العمل تحول إلى مصدر مدرّ للمال، إذ تتبع وتحلل سلوك الزبائن باستخدام هذه البيانات، مما يمنحها قوة هائلة في سوق الإعلانات، لتزويد الشركات بالمجموعات المستهدفة الأكثر ملاءمة لمنتجاتها وخدماتها.

بيانات للبيع

يذكر هوفمان الخبير المختص في التكنولوجيا أن مضاد الفيروسات أفاست يجمع نشاطات رواده ويقدمها إلى المسوقين من خلال شركة تدعى "جامبشوت". يمكن للشركات التي تدفع للبرنامج أن تطلع على بيانات تصفح المستخدمين كاملة لمعرفة ما يميلون إليه.

وقال مايكل كان وهو من موقع "بي. سي ماغ"، "تعدّ البيانات التي تجمعها الشركة دقيقة بحيث يمكن للزبائن أن يطلعوا على كل ما يقوم به المستخدمون عند تصفح الإنترنت بالملي/ ثانية. وعلى الرغم من أن البيانات لا توفر اسم صاحبها أو بريده الإلكتروني أو عنوان بروتوكول الإنترنت الخاص بكمبيوتره "آي.بي"، إلا أن كل سجل مستخدم يدرج تحت معرف يسمى معرف الجهاز، والذي يستمر إثراؤه إلى أن يقرر المستخدم إلغاء اعتماده على برنامج مضاد الفيروسات أفاست".

وفي ردها على التحقيق تقول شركة أفاست إن هذه البيانات تبقى "مجهولة المصدر". لكن، فريق "بي.سي ماغ" و"ماذربورد" أكدا أن هذه البيانات ليست مجهولة المصدر، وأن "ماذر بورد" تمكّن من ربط البيانات بالأفراد. كاشفا أنه على سبيل المثال، "إذا كنت تعرف أي مستخدم اشترى منتجا معينا من أمازون في وقت معين في تاريخ محدد، فسيمكنك تحديد الفرد "المجهول الهوية " ومن ثم الاطلاع على سجله".

صيد البيانات

يوضح التقرير أن أفاست اعتمد طريقة محددة لجمع المعطيات وذلك عبر برنامج مكافحة الفيروسات المصمم للكمبيوترات، وهي فرصة مناسبة وجدها برنامج الحماية لصيد بيانات الزبائن.

وشرح مايكل كان "إذا كنت تعتمد أفاست بالإعدادات 'الموصى بها'، فاعلم أن 'جامبشوت' باع بياناتك إلى المسوقين". مشيرا إلى أنه لا يتم جمع هذه البيانات من خلال ملحق البرنامج الخاص بالمتصفح "مثل كروم"، بل يتم جمعها من خلال التطبيق المصمم لأجهزة الكمبيوتر.

وأوضح كان أنه عند تثبيت أفاست، ستظهر نافذة تسألك عما إذا كنت ترغب في مشاركة بياناتك. مبينا أنه في واقع الأمر "حيلة لم يدرك معظم الأشخاص الذين نقروا على 'أوافق' ما وافقوا عليه".

ونبه الخبير التكنولوجي إلى أنه "إذا قررت مواصلة استخدام البرنامج، يمكنك فتح التطبيق والتوجه إلى القائمة "الإعدادات، العام، الخصوصية"، وذلك للتحكم في نوعية البيانات التي يتم جمعها ومشاركتها". وتابع "لكننا نوصي بالتخلي عن البرنامج كاملا واعتماد بديل لا يبيع بياناتك".

غالبا ما يحرص برنامج مكافحة الفيروسات على فرض الملحق المصمم للمتصفح على جمع بيانات مفصلة عن المستخدمين لأغراض تسويقية لفائدة الشركات العالمية التي تستخدم هذه المعلومات لصالح منتجاتها.

وتشمل المعلومات والبيانات التي تبيعها الشركة المذكورة معلومات عن عمليات البحث التي يقوم بها المستخدمون عبر أجهزتهم، ومواقع وإحداثيات الأجهزة التي قاموا بالبحث منها، إضافة إلى بيانات تتعلق بالمواقع التي يزورونها ومقاطع الفيديو التي يشاهدونها عبر يوتيوب.

ويرى الخبراء أن الهدف من شراء هذه البيانات بالنسبة إلى الشركات هو معرفة ما يفضله المستخدمون، وتوجيه الدعايات لهم وفقا لأهوائهم. وفي أكتوبر 2019، عمل مبتكر ملحق منع الإعلانات الشهير "أد بلوك بلس"، فلاديمير بالانت،على فهرسة الطريقة التي تجمع بها العديد من ملحقات أفاست البيانات وتنقلها. ولاحظ نفس الشيء عند تدقيقه في "أي.في.جي". ولا يعدّ الأمر مفاجئا، حيث استحوذت شركة أفاست على شركة حماية البرمجيات أي.في.جي في صفقة قيمتها 1.3 مليار دولار قبل سنوات.

الملحق جزء من المشكلة

وقررت إدارة موزيلا وغوغل حذف إضافات تابعة للشركتين بعد أن تأكدتا من تورطهما في التجسس على المستخدمين حتى أجرت إدارة أفاست بعض التغييرات مما جعلها متاحة للتنزيل مرة أخرى. وأصبحت الشركة أكثر "شفافية" في سياسة الخصوصية التي تعتمدها.

بينما يمكن أن تتخذ شركات المتصفحات إجراءات صارمة بشأن ما يمكن أن تنفذه شركة مضادات الفيروسات، فإنه لا يمكن لأحد أن يمنع شركة مثل أفاست من جمع البيانات باستخدام التطبيق المصمم لأجهزة الكمبيوتر. لذلك، لا يمكنك تجنب مشاكل الخصوصية عبر حذف ملحق أفاست من المتصفح الذي تعتمده.

في خضم ذلك يطرح خبراء التكنولوجيا تساؤلات بشأن كيفية حصول برامج مكافحة الفيروسات المجانية على مصادر لجمع الأموال وتحقيق الأرباح بطريقة أو بأخرى. لذلك، يرى بعضهم أنه من الضروري أن تتحول "شركات مثل أفاست إلى جمع بيانات الزبائن لجني الأموال منها".

وفي الماضي، قررت إدارة أفاست دمج ميزة "التسوق" التي أضافت إعلانات إلى صفحات الويب أثناء تصفح المستخدمين لها. لكن حاليا لم يعد البرنامج يفعل ذلك، لكنه تحول إلى عملية جمع للبيانات.

كما أشرنا في سنة 2015، لم تعد برامج مكافحة الفيروسات المجانية "مجانية" بحق. بل تحولت العديد من شركات مكافحة الفيروسات إلى تغيير محرك البحث الافتراضي الذي اختارته، واحتلال صفحة المتصفح الرئيسية، ودمج "عروض" لزبائنها. واليوم، من المرجح أن تكون العديد من تطبيقات مكافحة الفيروسات الأخرى متورطة في بيع البيانات التي تجمعها من مختلف المستخدمين الذين يعتمدون عليها لحمايتهم من مخاطر الويب.

غير أن التورط في بيع البيانات من قبل التطبيقات المجانية لا يدفعنا إلى أن نتّهم كل مضاد فيروسات مجاني بالضلوع في هذه الممارسات، باعتبار أنه لم يتسن لنا أن نفحص كل برامج مكافحة الفيروسات، وقد يوفر البعض نسخة تجريبية مجانية لا تجمع البيانات لتبيعها، حيث تحاول بيع منتجها مما يجعلها تعمل على ترغيبك فيه حتى تقبل بدفع مبلغ مقابل النسخة الكاملة.

على سبيل المثال، قال فلاديمير بالانت، ردا على من قالوا إنه لم يعثر على أي دليل يشير إلى أن برنامج مكافحة الفيروسات المجاني كاسبرسكي يتجسس على مستخدميه، إنه بقي غير مقتنع بالنهج الأمني الذي يتبعه مبرمجو الشركة.

ونصح بالانت باستخدام برنامج ويندوز ديفندر من مايكروسوفت التي دمجته في ويندوز 10، بما أن برنامج مكافحة الفيروسات التابع له لا يعمل على تحقيق أهداف تتجاوز مهاجمة البرامج الضارة التي يمكن أن تصيب الأجهزة. كما تقدّم مايكروسوفت عقود برامج أمن أكثر تقدما للشركات.

وخلص إلى أنه يوصي باستخدام مالويربايتس، الذي وجد أنه يكتشف البرامج غير المرغوب فيها لإزالتها، فيما تجني الشركة أموالها من اشتراكات بعض المستخدمين الذين يدفعون مقابل خدمات البرنامج كاملة بدلا من تتبع بيانات الجميع.

لا شيء مجانيا

في بيتنا جاسوس

أنيك جيسدانون

نيويورك - هل أدخل شخص ما جاسوسا إلى منزلك خلال العطلات؟ ربما...إذا أهداك أحد الأصدقاء أو أحد أفراد الأسرة سماعات تتفاعل بالصوت أو بعض الأجهزة الذكية الأخرى.

ولكن كل هذه الأجهزة بدءًا من السماعات المتصلة بالإنترنت مع المساعدين الصوتيين مثل "أمازون أليكسا" إلى أجهزة التلفزيون المزودة بنتفليكس يمكن أن تكون دائمة التنصت والاستماع والمشاهدة أحيانا أيضا. وكما هو الحال مع جميع التقنيات الجديدة تقريبا، يعني اقتناء هذه الأجهزة الموازنة بين مخاطر الخصوصية ووسائل الراحة التي تقدمها.

وتقدر شركة الأبحاث "آي.دي.سي" ازدياد كمية الشحنات في جميع أنحاء العالم إلى 815 مليون سماعة ذكية وكاميرات أمنية وغيرها من الأجهزة في عام 2019، بزيادة 23 بالمئة عن عام 2018. كان العديد من هذه المبيعات للهدايا.

يمكنك تجنب المخاطر تماما من خلال إعادة هذه الأجهزة على الفور. لكن إذا قررت الاحتفاظ بها، فهناك بعض الأشياء التي يمكنك القيام بها لتقليل احتمال هذا التنصت.

تتيح لك السماعات الذكية مثل "أمازون إيكو"، و"غوغل هوم" معرفة الطقس والمواعيد باستخدام أوامر صوتية بسيطة. بعض الإصدارات الحديثة تأتي مع الكاميرات والشاشات.

وتستمع العديد من هذه الأجهزة باستمرار للأوامر وتتصل بخوادم الشركات لتنفيذها. وعادة ما يتجاهلون الثرثرة الخاصة وينقلون التسجيلات الصوتية فقط عند تشغيل الجهاز.

ولكن لا توجد هناك طريقة سهلة للمستهلكين للتحقق من تلك الضمانات. حيث في إحدى الحالات، استمع مساعد "أليكسا" في جهاز "إيكو" عن طريق الخطأ إلى محادثة وثرثرة خلفية وعمل على تحويلهما إلى معلومات. بل أنه يمكن تخزين الأوامر الصوتية المرسلة عبر الإنترنت إلى أجل غير مسمى وقد تتضمن محادثات في الخلفية يمكن البحث عنها في الدعاوى القضائية والتحقيقات.

تتيح لك الشركات ذات السمعة الطيبة مراجعة وحذف صوتك، حيث تتيح لك "أمازون" الآن طلب الحذف التلقائي بعد 3 أو 18 شهرًا، لكنك بحاجة إلى إعداد هذا الخيار، ولا يوجد خيار لمنع "أمازون" من حفظ سجل أوامرك على الإطلاق.

وحتى وقت قريب، سمحت شركات التكنولوجيا للموظفين بمراجعة التفاعلات الصوتية من أجل مراقبة الجودة، وتم تسريب بعض هذه التفاصيل. وبعد رد الفعل العكسي، تقوم العديد من الشركات بجعل الأمر أكثر وضوحًا وأسهل من خلال استثناء المراجعة البشرية. وإذا كان لديك أطفال، فقم بإعداد رمز مرور للتسوق إذا كانت السماعات الخاصة بك تسمح بذلك، وإلا فسيكون الجهاز مجرد لعبة لطفلك.

أما بالنسبة للإصدارات التي تأتي بشاشة، فهناك العديد من الكاميرات الخاصة بمحادثات الفيديو. عندما لا تستخدم الجهاز، فكر في قلبه لمواجهة الجدار، خاصة في غرفة النوم والأماكن الخاصة الأخرى. أو غطي الكاميرا بأي شيء.من المفترض ألا تعمل في ذلك الوقت، ولكن كن حذراً.

تتيح لك كاميرات الحماية المتصلة بالإنترنت إمكانية مشاهدة حيواناتك الأليفة أو أطفالك عندما لا تكون في المنزل. يتيح لك أيضا برنامج "أمازون رينغ" التحقق ممن يقف عند باب منزلك دون الحاجة إلى القيام بهذا الدور بنفسك.

لم يعد المرء سيدا في بيته

ولكن المشكلة تكمن في أنه إذا كان بإمكانك مشاهدة الفيديو على أحد التطبيقات، فإنه يمكن للقراصنة الإلكترونيين أن يفعلوا ذلك أيضا بكل سهولة.

عندما تستخدم نفس كلمة المرور في خدمات متعددة، يمكن لهذا القرصان الذي يسرق كلمة المرور الخاصة بك من مكان واحد أن يجربها على خدمة الكاميرا أيضا. لذلك لا تعد استخدام كلمة المرور، ولكن حاول كذلك استخدام الخاصية التي تطلب منك إدخال رمز مؤقت تم إرساله كنص لضمان أنه أنت المستخدم.

ومرة أخرى، قد ترغب في تحويل الكاميرا لمواجهة الجدار عندما تكون في المنزل. إنه أمر مؤلم، وإذا نسيت أن تعيد وضعيتها مرة أخرى عند المغادرة، فإن ذلك يلغي غرض امتلاك كاميرا أمنية.

تتيح لك الأقفال الذكية فتح الأبواب من خلال استخدام تطبيق، حتى أنه يمكنك أن تسمح للضيوف بدخول المنزل عندما لا تكون فيه. وقد يحاول اللصوص اختراق هذا النظام، رغم أنه من الأسهل بالنسبة لهم في كثير من الأحيان مجرد كسر النافذة. وكإجراء وقائي، قم بتعطيل أي قدرات لإلغاء تأمين الأبواب من خلال إصدار أمر صوتي لسماعات ذكية، خاصة إذا كان لديك أطفال أشقياء، أو مراهقون قد يرغبون في التسلل إلى شخص ما.

وعلى الرغم من أن المفاتيح الرقمية يمكن أن تكون مريحة للسماح للضيوف بالدخول، إلا أنها يمكن أن تترك أثرا رقميا. وفي نزاع حول حضانة الأطفال، على سبيل المثال، قد يقوم زوجك السابق باستدعاء السجلات التي تخبره بأنك بقيت خارجاً إلى وقت متأخر في أيام المدرسة. وإذا قمت باستئجار شقة وأنشأت نسخة لأحد ضيوفك تُستخدم يوميًا، فقد يشك المالك في وجود شاغل غير مصرح به.

يوجد حل بسيط إذا كنت لا تستخدم ميزات الإنترنت على تلفزيونك الذكي: لا تقم فقط بتوصيل التلفزيون بشبكة واي فاي الخاصة بك في المقام الأول. وبالطبع، لن ينجح هذا إذا كنت لا تستخدم أداة منفصلة لبث الفيديو.

قد يحصل الأطفال على العديد من الدمى وغيرها من الألعاب التي يمكنها أن تتحدث. ولكن إذا كانت اللعبة متصلة بالإنترنت، فاحرص على التأكد من مقدار السيطرة التي تقع في أيدي الآباء، وما إذا كانت اللعبة تسمح للأطفال بالتواصل مع العالم الخارجي. يمكنك التحقق عبر الإنترنت لمعرفة ما إذا كان الآباء أو مجموعات المستهلكين الأخرى قد حددوا هذه المشكلات.