اقتصاد, تقنية وسيارات

18 أغسطس 2022 22:58 مساء

آلاف مستخدم واجهوا التهديدات المخبّأة في ملحقات متصفحات الويب 10

«دبي: «الخليج

(Browser Extensions). أجرى باحثو كاسبرسكي تحليلاً للأخطار التي تنطوي عليها ملحقات متصفحات الويب وشمل التحليل أنشطة مجرمي الإنترنت الذين يخفون تهديدات رقمية خطرة تحت ستار الوظائف الإضافية لتلك الملحقات. وتأثر أكثر من 10,000 مستخدم، مرة واحدة على الأقل، بالتهديدات المخبّأة في ملحقات المتصفحات في النصف الأول من العام 2022، ويمثل هذا العدد أكثر من 36.5% من عدد المستخدمين المتأثرين بهذا النوع من التهديدات طوال العام 2021 بأكمله. ويمكن للتهديدات الكامنة في ملحقات المتصفحات إدراج الإعلانات على أجهزة المستخدمين، وجمع البيانات منها حول سجلات التصفح وحتى البحث عن بيانات اعتماد تسجيل الدخول إلى مختلف الحسابات الخاصة، ما يجعلها من أكثر الأدوات المرغوب بها عند مجرمي الإنترنت، وذلك من خلال تقليد تطبيقات Video Downloader أو PDF Converter أو ملحقات ذات وظائف مفيدة مثل Google Translator شائعة مثل

واستطاعت منتجات كاسبرسكي، منذ بداية العام 2020، منع ما يقرب من 6 ملايين مستخدم من تنزيل تهديدات

متخفية تحت ستار ملحقات وهمية لمتصفحات الويب. وتمثّل التهديد الأبرز الذي انتشر تحت ستار ملحقات المتصفحات في برمجيات الإعلانات، التي تُعدّ برمجيات غير مرغوب فيها مُصمّمة لإظهار الإعلانات على الشاشة. وعادةً ما تستند هذه الإعلانات إلى سجل التصفح لجذب اهتمام المستخدمين عبر تضمين لافتات إعلانية في صفحات الويب أو توجيه تلك الصفحات إلى صفحات تابعة للقائمين خلف هذه الإعلانات، ما يمكّنهم من كسب المال. ولاحظ خبراء كاسبرسكي أن أكثر من 26,000 مستخدم فريد واجهوا بين يناير 2020 ويونيو 2022، برمجيات إعلانية مختبئة في ملحقات المتصفحات، أي أن نحو 81% من جميع المستخدمين المتأثرين قد واجهوا هذا التهديد.

يمكن برمجيات الإعلانات تتبع كل ما يبحث عنه المستخدم ثم الترويج لمنتجات متعلقة بالبحث عبر إعلانات تابعة على محرك البحث

وعُثر على إضافات خبيثة وغير مرغوب فيها يجري توزيعها من خلال الأسواق الرسمية. وكانت «جوجل» في العام 2020 Chrome. أزالت 106 ملحقات خبيثة من متجر الملحقات وتطبيقات الويب الخاص بمتصفحها واستُخدمت الملحقات المُزالة، والتي جرى تنزيلها حوالي 32 مليون مرة بالمجمل، في سرقة بيانات المستخدمين الحساسة، كملفات تعريف الارتباط وكلمات المرور، بل إن بعضها كان يصوّر لقطات لشاشات المستخدمين، ما عرض بيانات الملايين منهم للخطر.

لكن حدوث هذا الأمر لا يتكرّر كثيرًا، فالطريقة الرئيسة لتوزيع الملحقات الإضافية الخبيثة تتمثل في موارد الجهات الخارجية. وكانت إحدى عائلات التهديدات التي حللها باحثو كاسبرسكي وأوردوها في تقريرهم، والتي يطلق عليها اسم FB Stealer انتشرت فقط من خلال مواقع مشبوهة. وتُعتبر FB Stealer واحدة من أخطر عائلات التهديدات لأنها قادرة على سرقة بيانات اعتماد دخول المستخدمين من منصة «فيس بوك»، عدا عن قدرتها على تبديل محرك البحث التقليدي وتوجيه المستخدمين إلى صفحات تابعة.

أداة تثبيت برمجيات مخترقة، SolarWinds وعندما حاول المستخدمون أن ينزلوا من مصادر خارجية، مثل الموقع ذاتيًا على الجهاز FB Stealer الخطير، الذي قام بتثبيت NullMixer تلقوا تروجان Broadband Engineers مثل Google Translate. المصاب. وقد بدا الأمر طبيعيًا للمستخدمين، لأنه امتداده يحاكي امتداد التطبيق المألوف.

SolarWinds broadband engineers من خلال عدّة أدوات تثبيت، مثل NullMixer ينتشر تروجان استخراج ملفات تعريف الارتباط للمدة التي يعمل فيها FB Stealer ويمكن للتروجان بعد تشغيلkeymaker المستخدم على «فيس بوك»، وهي بمثابة الأسرار المخزنة في المتصفح والمشتملة على بيانات التعريف التي تسمح للمستخدمين بالبقاء في وضع تسجيل الدخول، وإرسالها إلى خوادم المهاجمين، ما يتيح لهم تسجيل الدخول فورًا إلى حساب المستخدم الضحية، حيث يكون بوسعهم، وبأسرع ما يمكن، محاولة طلب المال من أصدقائه الذين لا يدركون أن الحساب مخترق، وذلك قبل أن ينجح المستخدم في استعادة الوصول إلى حسابه.

إثراء تجربة المستخدم

وقال أنطون إيفانوف الباحث الأمني الأول لدى كاسبرسكي، إن الخطر قد يكمن حتى في ملحقات متصفحات الويب التي لا تحمل أية برمجيات خبيثة، موضحًا أن بيع مطوري هذه الملحقات بيانات المستخدمين المجمعة لجهات أخرى، مثلًا، من المحتمل أن يعرّضها لشخص ليس له حق الاطلاع عليها. وأضاف: «تحمل ملحقات متصفحات الويب الكثير

من المنافع التي تساهم في إثراء تجربة المستخدم على الإنترنت، كما إن بإمكان بعض الإضافات أن تجعل الأجهزة أكثر أمانًا، مثل أدوات إدارة كلمات المرور، لكن من المهم جدًا معرفة مدى سمعة المطوّرين وجدارتهم بالثقة، والحرص عند منح الأذونات التي تطلبها الملحقات. لذلك ستتضاءل فرصة مواجهة المستخدم للأخطار إذا اتبع توصيات «الاستخدام الآمن لملحقات المتصفحات».

لمعرفة المزيد حول الأخطار التي تنطوي عليها ملحقات Securelist يمكن الاطلاع على التقرير الكامل على متصفحات الويب الرسمية.

ويوصي خبراء كاسبرسكي المستخدمين باتباع التدابير التالية لحماية أنفسهم من تهديدات ملحقات المتصفحات:

استخدام المصادر الموثوق بها فقط لتنزيل البرمجيات، إذ غالبًا ما تُوزّع البرمجيات الخبيثة والتطبيقات غير المرغوب فيها عبر موارد جهات خارجية لم يتمّ التحقق من مدى سلامتها بالطريقة نفسها التي يجري بها التحقق من سلامة متاجر الويب الرسمية. وقد تثبّت هذه التطبيقات ملحقات خبيثة أو غير مرغوب فيها للمتصفحات من دون علم المستخدم، وقد يكون بوسعها تنفيذ أنشطة خبيثة أخرى.

تضيف الملحقات وظائف أخرى إلى المتصفحات، وتطلب منحها أذونات مختلفة للوصول إلى موارد الجهاز. لذا من المهم التدقيق في أهمية هذه الأذونات قبل منحها.

تحديد عدد الملحقات المستخدمة في المرّة الواحدة، ومراجعة الملحقات المثبتة مراجعة دورية لإلغاء تلك التي لم تعد مستخدمة أو غير المعروفة.

للتصفح الخاص، يمكن أن يساعد تجنب تتبع نشاط Kaspersky Internet Security استخدام حل أمني قوي مثل المستخدم على الإنترنت، وحمايته من التهديدات.