مايكروسوفت قدمت برنامج تشغيل محمل ببرامج ضارة

الاثنين 28 يونيو 2021 03:57 م

يلجأ صناع أنظمة التشغيل إلى توقيع التعليمات البرمجية لمساعدتك في الابتعاد عن البرامج الضارة، ولكن ربما تكون شركة مايكروسوفت قد كسرت عن غير قصد الثقة التي يهدف التوقيع إلى إنشائها.

وتوضح التقارير أن مايكروسوفت قد أكدت أنها وقعت على Netfilter، وهو برنامج تشغيل تابع لجهة خارجية لنظام التشغيل ويندوز يحتوي على برامج ضارة تم تداوله في مجتمع الألعاب.

ومر Netfilter عبر برنامج توافق أجهزة ويندوز WHCP. وكان يتصل بعناوين IP الصينية لخوادم القيادة والتحكم، كما وجد الباحث الأمني كارستن هان.

وقال هان: منذ ويندوز فيستا، يجب اختبار أي تعليمات برمجية يتم تشغيلها في وضع النواة وتوقيعها قبل الإصدار العام لضمان استقرار نظام التشغيل. ولا يمكن تثبيت برنامج تشغيل دون شهادة مايكروسوفت بشكل افتراضي.

وليس من الواضح كيف نجح البرنامج خلال عملية توقيع شهادة مايكروسوفت. وقالت الشركة: إنها تحقق في ما حدث وتقوم بتحسين عملية التوقيع وسياسات وصول الشركاء والتحقق من الصحة.

ولا يوجد دليل على أن مؤلفي البرنامج الضار قد سرقوا الشهادات، وامتنعت مايكروسوفت عن عزو هذا الحادث إلى جهات فاعلة في الدولة القومية حتى الآن.

وكان صانع برنامج التشغيل، Ningbo Zhuo Zhi، يعمل مع مايكروسوفت لدراسة وإصلاح أي ثغرات أمنية معروفة، بما في ذلك الأجهزة المتأثرة.

ويحصل المستخدمون على برامج تشغيل خالية من البرامج الضارة من خلال Windows Update.

مايكروسوفت تؤكد
قالت مايكروسوفت إن تأثير برنامج التشغيل محدود. وكان يستهدف اللاعبين، ولم يعرف عنه أنه عرض مستخدمي المؤسسة للخطر.

ولا يعمل برنامج التشغيل إلا بعد الاستغلال، وفقًا لما ذكرته مايكروسوفت. ويجب أن تكون قد حصلت على وصول على مستوى المسؤول على جهاز الحاسب لتثبيت برنامج التشغيل. وبمعنى آخر، لا ينبغي أن يشكل Netfilter تهديدًا.

ويرى العديد من الأشخاص أن برنامج التشغيل الموقَع يؤكد أن برنامج التشغيل أو البرنامج آمن.

وقد يتردد هؤلاء المستخدمون في تثبيت برامج تشغيل جديدة إذا كانوا قلقين من احتمال وجود برامج ضارة. حتى لو كانت برامج التشغيل هذه تأتي مباشرة من الشركة المصنعة.

وكشف هذا الحادث مرة أخرى عن تهديدات لأمن سلسلة التوريد للبرامج. إلا أنه نشأ هذه المرة عن ضعف في عملية توقيع التعليمات البرمجية لشركة مايكروسوفت.