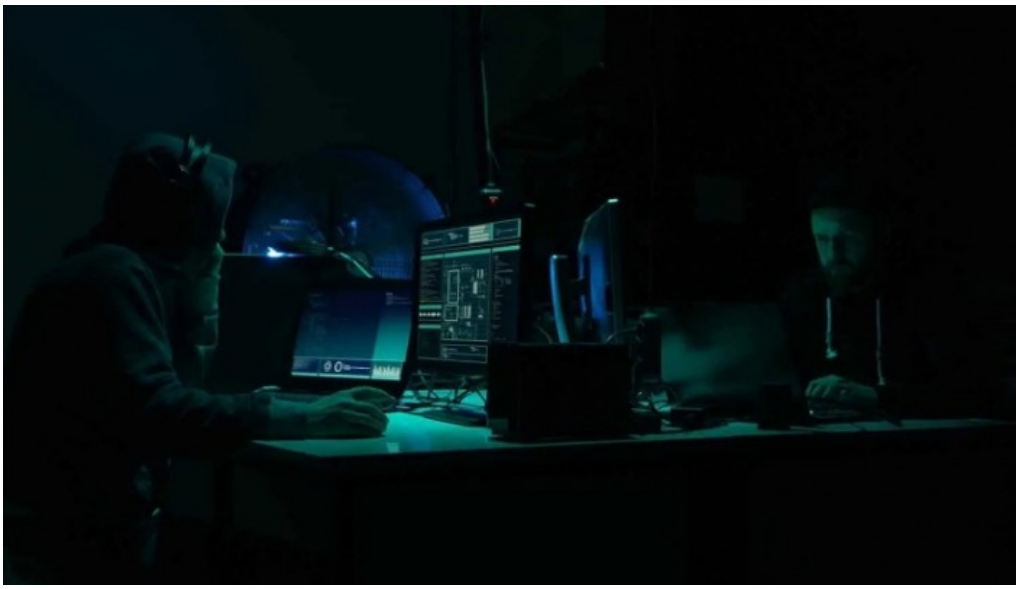
FBI يخترق مئات الحواسيب عن بُعد لحمايتها



الجمعة 16 أبريل 2021 11:05 م

في ما يُعتقد أنه خطوة غير مسبوقة، حاول مكتب التحقيقات الفيدرالي FBI حماية مئات أجهزة الحاسب المصابة باختراق Hafnium عن طريق اختراقها بنفسه، باستخدام أدوات المتسللين الأصلية.

وترك الاختراق، الذي أثر في عشرات الآلاف من عملاء Microsoft Exchange Server حول العالم وأثار استجابة حكومية كاملة من البيت الأبيض، عددًا من الأبواب الخلفية التي تسمح للمتسللين بالدخول إلى تلك الأنظمة مرة أخرى.

وبعد أشهر من استخدام المتسللين لأربع نقاط ضعف لم يتم اكتشافها سابقًا لمهاجمة آلاف الشبكات، استفاد مكتب التحقيقات الفيدرالي FBI من ذلك باستخدام الأبواب الخلفية نفسها لحذفها عن بُعد.

وتوضح وزارة العدل الأمريكية: أجرى مكتب التحقيقات الفيدرالي الإزالة عن طريق إصدار أمر من خلال الأبواب الخلفية إلى الخادم، الذي تم تصميمه لجعل الخادم يحذف الأبواب الخلفية فقط.

ومن المحتمل أن مالكي خوادم Microsoft Exchange هذه ليسوا على دراية بعد بتدخل مكتب التحقيقات الفيدرالي، ويقدم مكتب التحقيقات الفيدرالي خدمة للعالم من خلال إزالة تهديد مثل هذا.

وتقول وزارة العدل: إن الإعلان يقدم إشعار للمالكين بأن مكتب التحقيقات الفيدرالي FBI حاول مساعدتهم، وهو يفعل ذلك بموافقة كاملة من محكمة في تكساس.

وفي حين أن مايكروسوفت كانت بطيئة في استجابتها الأولية، فإن عملاء Microsoft Exchange Server كان لديهم أكثر شهر حتى الآن من أجل تصحيح الخوادم الخاصة بهم بعد عدة تنبيهات مهمة.

ويقول مكتب التحقيقات الفيدرالي FBI: تم تصحيح آلاف الأنظمة بواسطة مالكيها قبل أن نبدأ عملية إزالة الباب الخلفي عن بُعد لمجموعة القرصنة Hafnium.

وأضاف: أزلنا الأبواب الخلفية المتبقية لمجموعة القرصنة التي كان من الممكن استخدامها للحفاظ على الوصول المستمر وغير المصرح به إلى شبكات الولايات المتحدة.

وقالت وزارة العدل: إن العملية أزالت الأبواب الخلفية فقط، لكنها لم تصحح نقاط الضعف التي استغلها المتسللون.

ويشير البيان الصادر عن المدعي العام المساعد من قسم الأمن القومي بوزارة العدل: تُظهر الإزالة بإذن المحكمة للأبواب الخلفية الضارة التزام الوزارة بعرقلة نشاط القرصنة باستخدام جميع أدواتنا القانونية، وليس الملاحقات القضائية فقط.