الحرب السيبيرية على أمريكا

1 ما هي اهداف الاختراق؟

استهدفت الحملة وكالات الطاقة والخزانة والتجارة الامريكية، كما تعرضت مايكروسوفت للاختراق، وقالت شركة Solar Winds، التي تقف وراء البرنامج الذي استهدفه المتسللون، إن ما يصل إلى 18000 من أكثر من 300000 عميل قاموا بتنزيل البرنامج المخترق. كما تشمل قائمة الكيانات الحكومية الأمريكية المتضررة وزارة التجارة ووزارة الأمن الداخلي والبنتاغون ووزارة الخزانة وخدمة البريد الأمريكية والمعاهد الوطنية للصحة. تبدو الأهداف الى حد الان من وراء هذه الحملة، السعي الى الاستيلاء على الملكية الفكرية، والوصول إلى المعلومات الحساسة، ومراقبة أنشطة الحكومة الأمريكية، وتعطيل عمليات الحكومة الأمريكية.

2 كيف حصل الاختراق وأين؟

أدخل القراصنة برامج ضارة إلى أداة أمان الشبكة الشهيرة في Solar Wind والتي تسمى Orion، والتي تستخدمها العديد من الوكالات الحكومية والشركات الكبيرة، وقد بدأت العملية منذ شهر اذار/ مارس الماضي، حيث قام المتسللون بإرفاق برامجهم الضارة بتحديث برنامج من شركة Solar Winds، وهي شركة مقرها أوستن، تكساس. وتستخدم العديد من الوكالات الفيدرالية وآلاف الشركات في جميع أنحاء العالم، لمراقبة شبكات الكمبيوتر الخاصة بها. يعتقد خبراء الأمن السيبراني الذين أشاروا إلى الطبيعة المعقدة للغاية للهجوم، أن جهاز الاستخبارات الخارجية الروسي SVR، نفذ الاختراق. لكن خطورة الهجوم ودقته لا تستبعد تورط جهات أخرى في هذا الهجوم.

3 ماذا فعل المتسللون؟

قال جلين غيرستيل، المستشار العام السابق لوكالة الأمن القومي في الفترة من 2015 إلى 2020، "يبدو الأمر كما لو كنت تستيقظ ذات صباح وأدركت فجأة أن لصًا كان يدخل ويخرج من منزلك منذ ستة أشهر". استغل المتسللون الطريقة التي توزع بها شركات البرامج التحديثات، مضيفين البرامج الضارة إلى الحزمة الشرعية. ويبدو أنّ الشفرة الخبيثة تمنح المتسللين "بابًا خلفيًا" وموطئ قدم في شبكات الكمبيوتر والتي استخدموها بعد ذلك للحصول على معلومات حساسة.

4 كيف علّق "مايكروسوفت" على الاختراق؟

دعت مايكروسوفت إلى "استجابة عالمية للأمن السيبراني" في أعقاب الهجوم، وخصت بالذكر القطاع الخاص الإسرائيلي كمصدر محتمل للتهديدات، وقالت إن الحادث كان "هجومًا فعالًا على الولايات المتحدة وحكومتها والمؤسسات الهامة الأخرى. وإن عدد المواقع والأهداف المعروفة سيزداد مع استمرار التحقيق، وإنها عثرت على البرمجيات الخبيثة في أنظمتها الخاصة، وانّ هذا العمل، هو استهتار خلق ثغرة تكنولوجية خطيرة للولايات المتحدة والعالم. ."وأشار بيانها إلى أن القطاع الخاص في إسرائيل وشركة NSO Group الإسرائيلية يمثلان تهديدات محتملة. وأنّ مجموعة NSO كانت تشكّل تهديدًا جديدًا ومتطورًا لهجمات الأمن السيبراني المخصخصة، وانهم يشكّلون مرتزقة القرن الحادي والعشرين".

5 المخاطر

يشكّل الاختراق خطرا جسيما على الحكومات الفيدرالية وحكومات الولايات والحكومات المحلية، وعلى كيانات البنية التحتية الحيوية. انّ إزالة هذا الخطر سيكون معقدًا للغاية ويشكل تحديًا كبيرا وصعبا. لا يزال النطاق الحقيقي للاختراق غير معروف، ولكن يبدو أنه امتد إلى ما وراء الحكومة الأمريكية. من المستحيل التحكم الكامل في الضرر دون معرفة مدى الضرر - وسيستغرق تحديد من وما تم اختراقه بعض الوقت. ربما لم تكن SolarWinds هي نقطة الوصول الوحيدة، ولا يزال محللو الاستخبارات يحاولون تحديد ما تمكن المتسللون من استخلاصه من هذا الهجوم.

6 الإشكاليات والعوائق

أنفقت الولايات المتحدة مليارات الدولارات على أنظمة الأمن السيبراني والقدرات الهجومية الإلكترونية الجديدة لكنها لم تكن كافية لتجنب (أو اكتشاف) الخرق الأخير. عوائق كثيرة سيواجهها بايدن حول إمكانية تشكيل "وحدة أمن إلكتروني" غير قابلة للاختراق بحيث يتم حماية قرصنة الانتخابات والعديد من الأشياء السلبية الأخرى." قال بروس شناير، خبير أمني بارز وزميل في جامعة هارفارد: "لدينا مشكلة خطيرة، لا نعرف ما هي الشبكات التي يتواجدون فيها، ومدى عمقها، وما هي إمكانية الوصول التي لديهم، والأدوات التي تركوها". ليس من الواضح بالضبط ما الذي كان يبحث عنه المتسللون، لكن الخبراء يقولون إنه يمكن أن يتضمن أسرارًا نووية ومخططات لأسلحة متطورة وأبحاثًا متعلقة بلقاح فيروس كورونا ومعلومات لملفات عن قادة الحكومة وصناع القرار الرئيسيين.