الوكالات والشركات الأمريكية تؤمّن الشبكات الإلكترونية بعد حادثة اختراق ضخمة لها

مبنى وزارة المالية الأمريكية من نصب واشنطن، الأربعاء ـ 18 سبتمبر/أيلول 2019، واشنطن.

اخترق قراصنةٌ أجهزة الكمبيوتر في وزارة المالية الأمريكية، وربما وكالات فيدرالية أخرى، ما تسبّب في رد الحكومة على مجلس الأمن القومي. قال المتحدث باسم مجلس الأمن، جون أوليوت **John Ullyot**، يوم الأحد في 13 ديسمبر/كانون الأول 2020، إن الحكومة على علم بالتقارير المتعلّقة بعمليات الاختراق.

سارعت الوكالات الحكومية الأمريكية والشركات الخاصة يوم الاثنين 14 ديسمبر/كانون الأول لتأمين شبكات الكمبيوتر الخاصة بها بعد الكشف عن تجسسٍ إلكترونيٍّ متطورٍ وطويل الأمد يُشتبَه أنّ قراصنةً روس نفذوه. لم يتضح بعد المدى الكامل للضرر، لكن كان التهديد

المحتمل كبيرًا بما يكفي لدرجة أن وحدة الأمن الإلكتروني التابعة لوزارة الأمن الداخلي وجهت جميع الوكالات الفيدرالية لإزالة برامج إدارة الشبكات المخترقة، وكان من المتوقّع أن تفعل آلاف الشركات الشيء نفسه.

كان اللافت في العملية هو نطاقها المحتمل، وكذلك الطريقة التي تمكّن بها القراصنة من اختراق الدفاعات الإلكترونية والوصول إلى البريد الإلكتروني والملفات الداخلية في وزارة المالية والتجارة، وربما في أي مكان آخر. كان التّجسس دليلًا صارخًا على ضعف الشبكات الحكومية التي يُفترض أنها آمنة، حتى بعد الهجمات السابقة المعروفة.

قالت سوزان سبولدينج **Suzanne Spaulding**، المسؤولة السابقة في مجال الأمن الإلكتروني والتي تعمل الآن مستشارةً أولى في مركز الدراسات الاستراتيجية والدولية: "هذا تذكير بأن الهجوم أسهل من الدفاع، ولا يزال أمامنا الكثير من العمل للقيام به".

لا تزال هوية الجاني غير واضحة، كما قال مسؤول أمريكي، والذي تحدّث بشرط عدم الكشف عن هويته بسبب التحقيق الجاري، لوكالة أسوشيتد برس يوم الاثنين 14 ديسمبر/كانون الأول أن القراصنة الروس مشتبه بهم.

وصرّحت صحيفة واشنطن بوست نقلًا عن مصادر لم يُكشَف عنها إن الهجوم نفذه قراصنة تابعون للحكومة الروسية يطلقون على نفسهم الأسماء المستعارة **APT29** أو **Cozy Bear**، ويشكّلون جزءًا من أجهزة المخابرات الأجنبية لتلك الدولة.

ظهر الاختراق بعد أن صرّحت شركة الأمن الإلكتروني البارزة **FireEye** بأنها قد اختُرِقت، ونبّهت أن الحكومات الأجنبية والشركات الكبرى معرّضةً للخطر أيضًا، ولم تذكر الشركة من تشتبه به، رغم أن العديد من الخبراء يعتقدون أن روسيا مسؤولةً عن ذلك نظرًا لمستوى المهارة التي ينطوي عليها الأمر.

قال تشارلز كارماكال **Charles Carmakal**، نائب رئيس **FireEye**: إن الشركة كانت على دراية بـ "عشرات المستهدفين ذوي القيمة العالية والذين قد اخترقهم القراصنة، وكانت تساعد بشكلٍ استباقيٍّ عددًا من المنظمات في الرد على التدخلات التي كانت تتعرض لها". وقال إنه يتوقّع أن يعلم في الأيام المقبلة أنهم تعرضوا للاختراق كذلك.

أقرّت السلطات الأمريكية بتأثر الوكالات الفيدرالية بحادثة الاختراق يوم الأحد 13 ديسمبر/كانون الأول، وقدّمت تفاصيلَ قليلةً. قالت وكالة الأمن الإلكتروني وأمن البنية التحتية، المعروفة باسم **CISA**، في توجيهٍ غير معتاد أن برنامج الشبكة المستخدم على نطاق واسع **SolarWinds** قد تعرّض للاختراق، ويجب إزالته من أي نظام يستخدمه. وأصدرت وكالات الأمن الإلكتروني الوطنية في بريطانيا وأيرلندا تنبيهاتٍ مماثلةً.

تستخدم مئات الآلاف من المنظمات حول العالم **SolarWinds**، بما في ذلك معظم شركات **Fortune 500**، والعديد من الوكالات الفيدرالية الأمريكية.

تمكّن القراصنة من إرفاق برامجَ ضارّةٍ ضمن تحديث أمني صادر عن الشركة، ومقرها أوستن، تكساس.

على الرغم من أن **SolarWinds** تشير إلى تعرّض 18,000 عميل لتلك البرامج على أجهزتهم الإلكترونية، فإن معظم البرامج الضارّة لم تُنشَّط. عندما كان الأمر كذلك، كان بإمكان القراصنة انتحال صفة مسؤولي النظام والوصول الكامل إلى الشبكات المخترقة.

أضاف كارماكال إن القراصنة منضبطون للغاية، على الرغم من ارتكابهم أخطاء قليلة في إخفاء وجودهم في الشبكات، فقد اختاروا فقط

أهدافًا ذات معلوماتٍ مرغوبةٍ للغاية، لأنه في كل مرة ينشّطون فيها الأداة عن بُعد، تزداد احتمالية الكشف عن هويتهم.

قال بن جونسون **Ben Johnson**، وهو عضو سابق في وكالة الأمن القومي ومهندس إلكتروني وهو الآن كبير مسؤولي التكنولوجيا في شركة **Obsidian** لأمن البرمجيات: "بصراحةٍ تامةٍ، غرق قلبي عندما رأيت بعض التفاصيل، فقط مقدار المعلومات التي يمكن أن يحصلوا عليها إذا كانوا يقرؤون رسائل البريد الإلكتروني للجميع، ويصلون إلى ملفاتٍ حساسةٍ داخل أماكن مثل وزارة المالية أو التجارة".

قالت شركة **SolarWinds** إن عملاءها يشملون جميع الفروع الخمسة للجيش الأمريكي، والبنتاغون، ووزارة الخارجية، ووكالة ناسا، ووكالة الأمن القومي، ووزارة العدل، والبيت الأبيض، إلى جانب أكبر شركات الاتصالات والمحاسبة الأمريكية.

صرّح المتحدث باسم مجلس الأمن القومي جون أوليوت يوم الاثنين 14 ديسمبر/كانون الأول إن إدارة ترامب تعمل مع CISA ووكالات المخابرات الأمريكية ومكتب التحقيقات الفيدرالي والإدارات الحكومية المتضررة من التدخل لتنسيق الرد.

قال كريس بينتر **Chris Painter** الذي نسّق السياسة الإلكترونية في وزارة الخارجية خلال إدارة أوباما: "من الواضح أنها مهمة وواسعة النطاق بشكل لا يصدق". وأضاف :"ما مقدار ما اختُرِق؟ كم سُرِّب؟ هناك الكثير من الأسئلة المفتوحة الآن". وقال المتحدّث باسم الكرملين ديمتري بيسكوف **Dmitry Peskov** يوم الاثنين 14 ديسمبر/كانون الأول إن روسيا "لا علاقةَ لها" بالاختراق.

وقال بيسكوف للصحفيين: "مرةً أخرى يمكنني دحض هذه الاتهامات". أضاف: "إذا لم يستطع الأمريكيون فعل أي شيء حيال ذلك لعدة أشهر، فعندئذٍ، على الأرجح، لا ينبغي لأحد أن يلوم الروس من دون سبب على كل شيء".

لطالما كانت الوكالات الفيدرالية أهدافًا جذابةً للقراصنة الأجانب الذين يتطلعون إلى اكتساب نظرةٍ ثاقبةٍ لموظفي الحكومة الأمريكية وصنع السياسات.

على سبيل المثال، تمكن قراصنة مرتبطون بروسيا من اقتحام نظام البريد الإلكتروني لوزارة الخارجية في عام 2014، ما أدّى إلى اختراقه بشكلٍ كاملٍ لدرجة أنه كان لا بدّ من قطعه عن الإنترنت بينما عمل الخبراء على القضاء على ذلك الاختراق.

بعد ذلك بعام، تسبب اختراقٌ في مكتب شؤون الموظفين التابع للحكومة الأمريكية أُلقي باللوم فيه على الصين في اختراق المعلومات الشخصية لنحو 22 مليون موظف فيدرالي حالي وسابق ومحتمل، بما في ذلك البيانات الحساسة للغاية مثل التحقيقات السرية. قال خبراء الأمن الإلكتروني إن الهدف من الجهود التي استمرت لأشهر يبدو أنه التجسس وليس الربح أو إلحاق الضرر.

قال بن بوكانان **Ben Buchanan**، خبير التجسس الإلكتروني بجامعة جورج تاون، إنه من حيث الحجم وحده، تبدو العملية مشابهة للاختراق 2105 لمكتب إدارة شؤون الموظفين الذي تلقي السلطات باللوم فيها على الحكومة الصينية.

قال بوكانان، مؤلّف كتاب "**The Hacker and The State**": "هؤلاء من ذوي الخبرة والقدرة، وماهرون في العثور على نقاط ضعف نظامية في الاجهزة ومن ثم استغلالها بهدوء لعدة أشهر".

كان أعضاء الكونجرس يضغطون على الحكومة للحصول على مزيد من المعلومات. قال السناتور رون وايدن **Ron Wayden**، وهو ديموقراطي من ولاية أوريغون له صوت بارز في قضايا الإنترنت: "إذا كانت التقارير صحيحةً، وكان القراصنة الذين ترعاهم الدولة قد

تسللوا بنجاح إلى برامج مليئة بالبرمجيات الخبيثة إلى عشرات أنظمة التابعة للحكومة الفيدرالية، فقد عانى بلدنا من فشلٍ هائلٍ للأمن القومي قد يكون له تداعيات لسنوات قادمة".

إذا نفّذته حكومةٌ أجنبية، ولدى الولايات المتحدة الدليل، فسيصبح السؤال عمّا يجب فعله حيال ذلك.

قد تشمل بعض الخيارات الواضحة طرد الدبلوماسيين من الدولة المخالفة، وفرض عقوبات أو توجيه اتهامات جنائية بالتجسس الإلكتروني، وهي خطوات اتخذتها واشنطن والاتحاد الأوروبي ضد روسيا في الماضي.

وقالت سبولدينج: "أنا متأكدة من أن إدارات مثل **NSA** و**Cyber Command** تبتكر خيارات، وأن وزارة المالية تبحث في خيارات العقوبات، وأن وزارة الخارجية تبحث عن الكيفية التي سترسل بها إشارة قوية". أضافت: "ويبقى أن نرى ما إذا كانوا سيحصلون على موافقة على كل هذه الأشياء من البيت الأبيض".

في غضون ذلك، كانت **SolarWinds** والعديد من عملائها من القطاع الخاص يعملون على إغلاق أي خروقات وإصلاح الأضرار.

قالت الشركة في ملف مالي إنها تعتقد أن أقل من 18,000 عميل ثبتوا تحديث المنتج المخترق في وقتٍ سابقٍ من هذا العام.

قال جون هولتكويست **John Hultquist**، مدير تحليل في **FireEye**: "نتوقّع أن يكون هذا حدثًا كبيرًا للغاية عندما تظهر جميع المعلومات".

- التاريخ: 2020-12-27
- التصنيف: تكنولوجيا

#اختراق #الشبكات الإلكترونية #مجلس الأمن #المخابرات

المصادر

- Techxplore

المساهمون

- ترجمة
  - لوتيسيا هيثم يوسف
- مُراجعة
  - سارة صالح
- تحرير
  - رأفت فياض

- تصميم
  - روان زيدان
- نشر
  - روان زيدان