العرب
الإثنين 2020/12/21
السنة 43 العدد 11918

الولايات المتحدة مرتبكة أمام «أم الاختراقات» السيبرانية

إدارة بايدن تتوعد بالرد المناسب بعد نفاذ جواسيس أجانب إلى أسرار جهات حكومية أميركية

مازال نطاق الهجوم الإلكتروني الكبير الذي استهدف الولايات المتحدة يتوسع مع اكتشاف ضحايا آخرين خارج البلد، ما يجدد المخاوف إزاء مخاطر التجسس ويثير الريبة تجاه روسيا التي توجه إليها أصابع الاتهام. وأوضحت وكالة رويترز في تقرير جديد الأحد أن الاختراق السيبراني الأخير هو الأخطر على الإطلاق حيث أصاب الوكالات الحكومية الأميركية، ما من شأنه أن يربك إدارة الرئيس المنتخب جو بايدن، الذي توعد بالرد المناسب، فيما يحذر خبراء من التهديد الذي يحمله هذا الهجوم على الأمن القومي، ليس فقط في حال السيطرة على بنى تحتية حساسة، ولكن أيضا في حال النفاذ إلى إدارة شبكات توزيع الكهرباء أو خدمات عامة أخرى.

كريستوفر بينج/ جاك ستابز

واشنطن – خلال عشاء خاص لكبار التنفيذيين في قطاع الأمن التكنولوجي بفندق سانت ريجيس في سان فرانسيسكو، أبدى رئيس وكالة الأمن القومي والقيادة السيبرانية في الولايات المتحدة تفاخره في أواخر فبراير الماضي بمدى تمكن مؤسساته من حماية البلاد من الجواسيس.

ويروي صحافي من رويترز كان حاضرا في ذلك العشاء يوم 26 فبراير أن الجنرال بول ناكاسوني، وهو المسؤول الأول عن الأمن السيبراني في الولايات المتحدة، قال إن الفرق الأميركية "تفهم الخصوم أكثر مما يفهم الخصوم أنفسهم".

ومع ذلك، فقد كشف تسلسل زمني نشرته شركة مايكروسوفت وأكثر من عشرة باحثين من الحكومة والقطاع الخاص أنه بينما كان الجنرال يلقي كلمته كان متسللون يزرعون برنامجا خبيثا في شبكة تابعة لشركة برمجيات في تكساس اسمها "سولار ويندز كورب".

وبعد انقضاء ما يزيد قليلا على ثلاثة أسابيع من ذلك العشاء، بدأ المتسللون عملية مخابراتية كاسحة اخترقت قلب الحكومة ومؤسسات عديدة في الولايات المتحدة ومؤسسات أخرى في مختلف أنحاء العالم.

وانكشفت نتائج تلك العملية يوم 13 ديسمبر الجاري عندما ذكرت رويترز أن متسللين يشتبه أنهم روس استطاعوا النفاذ إلى البريد الإلكتروني الخاص بوزارتي الخزانة والتجارة الأميركيتين.

ومنذ ذلك الحين، يقول مسؤولون وباحثون إنهم يعتقدون أن ما لا يقل عن ست وكالات حكومية أميركية تعرضت للاختراق وأن البرنامج الخبيث أصاب الآلاف من الشركات فيما يبدو أنها واحدة من أكبر عمليات الاختراق التي تم الكشف عنها.

وقال وزير الخارجية الأميركي مايك بومبيو، الجمعة، إن روسيا تقف وراء هذا الهجوم الذي وصفه بأنه "خطر جسيم" على الولايات المتحدة. فيما نفت روسيا أن لها دورا في الهجوم.

ويأتي الكشف عن الهجوم في وقت صعب تتصدى فيه الحكومة الأميركية لفترة انتقالية بين رئيسين تشوبها الخلافات وأزمة متفاقمة على صعيد الصحة العامة.

كما يعكس الهجوم مستوى جديدا من حيث تطوره ومداه، إذ شمل وكالات اتحادية عدة وهدد بإلحاق ضرر أكبر بالثقة العامة في البنية التحتية الأميركية في مجال الأمن السيبراني مقارنة بأي عمليات تجسس إلكتروني سابقة.

ولا يزال جانب كبير من هذا الضرر مجهولا حتى الآن وكذلك الدافع والهدف النهائي وراء الهجوم.

وأوضح سبعة مسؤولين بالحكومة أنهم يجهلون إلى حد كبير ما هي المعلومات التي ربما تعرضت للسرقة أو التلاعب أو ما هو المطلوب لمعالجة الضرر.

> فلاديمير بوتين
>
> **جهاز المخابرات الخارجية يقوم بدور استثنائي لحماية البلاد**

واستغرق حل اللغز سنوات في آخر مرة يُشتبه أن النظم الاتحادية الأميركية تعرضت فيها للاختراق من جانب المخابرات الروسية، وذلك عندما استطاع متسللون النفاذ إلى نظم البريد الإلكتروني غير السرية في البيت الأبيض ووزارة الخارجية وهيئة الأركان المشتركة في العامين 2014 و2015.

وهوّن الرئيس الأميركي دونالد ترامب، السبت، من عملية الاختراق وتورط روسيا فيها وأصر على أن الأمور "تحت السيطرة" وأن الصين ربما تكون وراء العملية. كما اتهم "إعلام الأخبار الزائفة" بالمبالغة في مدى الاختراق. غير أن مجلس الأمن القومي سلم بأن "حادثا سيبرانيا خطيرا" قد وقع.

وقال جون أوليوت المتحدث باسم المجلس "سيكون هناك رد مناسب على أولئك المسؤولين عن هذا التصرف". ولم يرد على سؤال عما إذا كانت لدى ترامب أدلة على تورط الصين في الهجوم.

وقد أصدرت عدة وكالات حكومية منها وكالة الأمن القومي ووزارة الأمن الداخلي بيانات تقنية عن الوضع، فيما امتنع ناكاسوني عن التعليق.

وقال أعضاء في الكونغرس من الحزبين الجمهوري والديمقراطي إنهم يبذلون جهودا كبيرة للحصول على إجابات من الوزارات التي يشرفون عليها ومنها وزارة الخزانة.

وكشف أحد العاملين بمجلس الشيوخ أن رئيسه علم بتفاصيل عن الهجوم من وسائل الإعلام أكثر مما أطلعته عليه الحكومة.

ووفق ما هو معروف حتى الآن، نجح القراصنة في اختراق الرسائل الإلكترونية الداخلية لوزارة الخزينة ووزارة التجارة الأميركية، ويحتمل أنهم نفذوا إلى وزارة الطاقة التي تدير الترسانة النووية.

من جانبه أشاد الرئيس الروسي فلاديمير بوتين الأحد، بالجواسيس الروس "الشجعان" في الذكرى المئوية لتأسيس جهاز الاستخبارات الخارجية الروسي. لافتا إلى أن جهاز المخابرات الخارجية يقوم بدور استثنائي لحماية البلاد، وذلك في تصريحات أدلى بها بعد وقت قصير من اتهام البعض لموسكو بوقوفها خلف هجوم شامل على مؤسسات الحكومة الأميركية.

وقال بوتين في كلمة ألقاها أمام مقر جهاز الاستخبارات الخارجية في موسكو "أتمنى النجاح لكل من يدافع عن روسيا وعن شعبنا ضد التهديدات الخارجية والداخلية، ويدافع عن سيادتنا ومصالحنا الوطنية".

وتابع "أعرف جيدا أن هؤلاء أشخاص مخلصون وشجعان يؤدون خدمتهم" في صفوف جهاز الاستخبارات الخارجية الذي خلف الاستخبارات السوفييتية (كيه.جي.بي).

وفي خروج نادر، وضع بوتين الذي كان عميلا في الاستخبارات السوفييتية، إكليلا من الزهور عند قاعدة النصب التذكاري الذي تم تدشينه أمام مقر جهاز الاستخبارات الخارجية الذي يحتفل بالذكرى المئوية لتأسيسه هذا العام.

مهارات تجسس قوية

انكشفت عملية الاختراق الأسبوع الماضي عندما كشفت شركة فاير آي الأميركية للأمن السيبراني أنها تعرضت هي نفسها لهجوم سيبراني من النوع ذاته الذي يدفع لها زبائنها المال لمنعه.

وبدا في البداية أن الحادث كان في أغلبه مصدر حرج للشركة، غير أن اختراق شركات الأمن أمر له خطورته الخاصة لأن أدوات هذه الشركات غالبا ما تكون متصلة بأعماق نظم الكمبيوتر لدى مشتركيها.

وقبل أيام من الكشف عن الاختراق، علم باحثو الشركة أن أمرا غير عادي يحدث واتصلوا بشركة مايكروسوفت ومكتب التحقيقات الاتحادي، وذلك وفقا لما قالته ثلاثة مصادر كانت طرفا في هذه الاتصالات.

وكان فحوى الرسالة أن فاير آي تعرضت لحملة تجسس سيبرانية متطورة على نحو استثنائي نفذتها دولة وأن مشاكلها ربما تكون مجرد قمة جبل جليد يختفي تحتها الكثير.

وقال مصدران مطلعان إن حوالي ستة باحثين من فاير آي ومايكروسوفت بدأوا التحقيق في الأمر. وتوصلوا إلى أن أساس المشكلة كان شيئا يلقي الرعب في نفوس المتخصصين في الأمن السيبراني ويتمثل في استخدام تحديثات برمجية في تركيب برامج خبيثة يمكنها أن تتجسس على الأنظمة وتسرّب معلومات وربما تحدث أنواعا أخرى من الاضطراب.

وفي 2017 استخدم زبائن روس هذا الأسلوب في تعطيل نظم الكمبيوتر الخاصة والحكومية في مختلف أنحاء أوكرانيا بعد إخفاء برنامج خبيث اسمه "نوت بتيا" في برنامج يستخدم على نطاق واسع في المحاسبة. وككل مرة نفت روسيا تورطها في الأمر.

وسرعان ما انتشر البرنامج الخبيث في أجهزة الكمبيوتر في العشرات من الدول الأخرى وعطل شركات وتسبب في خسائر بمئات الملايين من الدولارات.

واستخدم الاختراق الأخير في الولايات المتحدة تقنية مماثلة.

فقد قالت سولار ويندز إن تحديثات برمجياتها تعرضت للانكشاف واستُخدمت في تركيب برنامج خبيث أصاب ما يقرب من 18 ألف نظام لدى زبائنها. وتستخدم مئات الألوف من المؤسسات برنامج أورايون الخاص بالشركة لإدارة الشبكات.

ويعطي البرنامج إشارة للمهاجمين بمجرد تنزيله عن موقعه. وفي بعض الحالات عندما تكون للولوج إلى الموقع أهمية خاصة يستغله المتسللون في نشر برامج خبيثة أخرى أنشط للانتشار في النظام المستهدف.

وفي بعض الهجمات جمع المتسللون بين امتيازات القائمين على إدارة النظم الممنوحة لشركة سولار ويندز ومنصة أزور السحابية التابعة لمايكروسوفت والتي تخزن بيانات الزبائن لصياغة بطاقة مصادقة للتحقق من الهوية. وأتاح ذلك للمتسللين إمكانيات في اختراق البريد الإلكتروني والوثائق أوسع بكثير مما تعتقد مؤسسات كثيرة أنه ممكن.

وقالت وكالة الأمن القومي الخميس في بيان إرشادي إنه كان بوسع المتسللين آنذاك سرقة الوثائق من خلال برنامج أوفيس 365 الذي توزعه شركة مايكروسوف وهو نسخة الإنترنت من أوسع برامجها استخداما في الأعمال. وأعلنت مايكروسوفت أيضا الخميس أنها عثرت على البرنامج الخبيث في نظمها.

وقال روب جويس أحد كبار مستشاري وكالة الأمن القومي في تغريدة على تويتر "هذه مهارات تجسس قوية وتحتاج لفهمها للدفاع عن الشبكات المهمة".

وليس من المعروف كيف أو متى بدأ النفاذ إلى نظم شركة سولار ويندز. ويقول باحثون في مايكروسوفت وشركات أخرى تحقق في الهجوم إن المتسللين بدأوا العبث ببرمجيات سولار ويندز في أكتوبر 2019 قبل بضعة أشهر من بدء الهجوم.

تقوية شبكاتنا

يتنامى الضغط على البيت الأبيض لاتخاذ إجراء ردا على هذا الاختراق الخطير. فقد قال السيناتور الجمهوري ماركو روبيو "لا بد للولايات المتحدة من الرد وليس بمجرد العقوبات". وشبه الجمهوري ميت رومني الهجوم بالسماح أكثر من مرة للقاذفات الروسية بالطيران فوق الولايات المتحدة دون رصدها.

أما السيناتور ديك دربن الديمقراطي فقد وصف الهجوم بأنه "إعلان حرب فعلي".

وقال ديمقراطيون من أعضاء الكونغرس إنهم لم يتلقوا معلومات تذكر من إدارة ترامب بخلاف ما نشر في وسائل الإعلام.

وامتنع أوليوت المتحدث باسم مجلس الأمن القومي عن التعليق على جلسات إطلاع أعضاء الكونغرس على الأمر. وقال في بيان لرويترز إن البيت الأبيض "يركز على التحقيق في الظروف المحيطة بهذا الحادث ويعمل مع شركائنا في مختلف الوكالات للتخفيف من وطأة الوضع".

وسيتعين على الرئيس الأميركي المنتخب جو بايدن مواجهة المشكلة عند توليه السلطة في 20 يناير القادم. وقال يوهانس أبراهام المدير التنفيذي لفريق بايدن الانتقالي للصحافيين، الجمعة، إنه سيكون هناك "ثمن باهظ" وإن الإدارة القادمة "ستحتفظ بحق الرد في الوقت الذي تختاره وبالأسلوب الذي تريده بالتنسيق مع حلفائنا وشركائنا في الأغلب".

وقال النائب الديمقراطي آدم شيف رئيس لجنة المخابرات بمجلس النواب إن على بايدن "أن يجعل من تقوية شبكاتنا والبنية التحتية العامة والخاصة أولوية رئيسية".

ويسلط الهجوم الضوء على تلك الدفاعات السيبرانية ويجدد انتقادات القائلين إن وكالات المخابرات الأميركية أكثر اهتماما بالعمليات السيبرانية الهجومية منها بحماية البنية التحتية الحكومية.

الاختراق الإلكتروني الأخطر في تاريخ الولايات المتحدة

ما هي وكالة الأمن القومي والقيادة السيبرانية في الولايات المتحدة؟

واشنطن – وكالة الأمن القومي هي هيئة مخابراتية تابعة لحكومة الولايات المتحدة، مسؤولة عن مراقبة وجمع ومعالجة المعلومات والبيانات لأغراض المخابرات والمخابرات المضادة وهو مجال معروف باسم مخابرات الإشارة.

بالتوازي مع ذلك، تعدّ وكالة الأمن القومي مسؤولة عن حماية اتصالات حكومة الولايات المتحدة ونظم معلوماتها ضد الاختراق وحرب الشبكات. ومع أن الكثير من برامج وكالة الأمن القومي تعتمد على الجمع الإلكتروني السلبي، إلا أن الوكالة مخولة بالقيام بمهامها بواسطة وسائل سرية نشيطة، من بينها إدخال وسائل مادية في النظم الإلكترونية، ويُدّعى عليها أيضًا تورطها في التخريب بواسطة البرمجيات التي أخضعتها.

بالإضافة إلى ما سبق، تحتفظ وكالة الأمن القومي بحضور مادي في عدد كبير من البلدان حول العالم، حيث تُدخل خدمة الجمع الخاصة لأجهزة تنصت في أماكن يصعب الوصول إليها. وتتضمن أساليب خدمة الجمع الخاصة "المراقبة عن قرب، والسرقة، والتنصت عبر الأسلاك، والاقتحام".

وتعتبر وظيفة التجسس لدى وكالة الأمن القومي جزءا لا يتجزأ من جهاز القوة العسكرية الأميركية. وهذا الجهاز العسكري يعمل داخل سياق التحالفات الاستراتيجية الأميركية، ومن بينها تحالفات عُقدت منذ سنة 1948، وأساسا مع المملكة المتحدة وكندا وأستراليا ونيوزيلندا.

● متى تأسست؟

يعود أصل الوكالة إلى وحدة أنشأت لفك شفرات الاتصالات في الحرب العالمية الثانية، وفي عام 1952 اتخذت اسمها الحالي إبّان عهد الرئيس هاري ترومان. ومنذ ذلك الحين، أصبحت الوكالة واحدة من أكبر هيئات المخابرات الأميركية من حيث عدد الأفراد والميزانية، عاملة ضمن وزارة الدفاع وترفع تقاريرها إلى مدير المخابرات الوطنية.

● مهام القيادة السيبرانية

تتجلى وظيفة القيادة السيبرانية في توحيد عمليات الفضاء الإلكتروني، وتعزيز قدرات الأمن المعلوماتي لوزارة الدفاع، وخبرتها في هذا المجال. وتم إنشاء القيادة الإلكترونية الأميركية في منتصف عام 2009 بمقر وكالة الأمن القومي.

وتنسق القيادة في عملها مع شبكات وكالة الأمن القومي، ويرأسها مدير وكالة الأمن القومي منذ إنشائها. وعلى الرغم من أن القيادة تم إنشاؤها في الأصل لأغراض دفاعية، إلا أنه يُنظر إليها على أنها قوة هجومية.

● دوافع الفشل

يُنظر إلى الولايات المتحدة على نطاق واسع على أنها القوة السيبرانية الأقوى في العالم. لكن مع ذلك لم تنجح في استباق محاولات الاختراق في السنوات الأخيرة التي وجهت فيها أصابع الاتهام إلى روسيا.

الأمن القومي الأميركي مهدد

وكانت الولايات المتحدة قد قررت في شهر سبتمبر 2018 اتخاذ موقف أكثر شراسة في الحرب السيبرانية، التي تتواجه فيها خصوصا مع الصين وروسيا ومنافسين آخرين، وقد أكد جون بولتون مستشار الرئيس الأميركي دونالد ترامب للأمن القومي السابق حينها أن "أول استراتيجية إلكترونية مفصلية بالكامل خلال السنوات الـ15" الماضية دخلت الآن حيّز التنفيذ. ومع ذلك لم تثبت الاستراتيجية الأميركية نجاعتها.

وبالنسبة إلى خصوم واشنطن، تشكل الهجمات السيبرانية والقرصنة الإلكترونية إحدى الطرق الفعالة والمدمرة التي يتم استغلالها لإلحاق الضرر بها دون عناء مقارنة بالهجمات المسلحة التي تتطلب مجهودات ومعدات ووقتا أكبر.

وتؤكد أوساط سياسية أميركية فشل واشنطن في حماية أمنها السيبراني وخاصة في السنوات الأخيرة.

وأوضحت صحيفة نيويوريك تايمز تعليقا على الاختراق الأخير، بأنه على مدار السنوات القليلة الماضية، أنفقت الحكومة الأميركية عشرات المليارات من الدولارات على قدرات التجسس الإلكتروني وبناء غرفة حرب عملاقة في فوت ميد، بولاية ميريلاند للقيادة الإلكترونية للولايات المتحدة، مع تثبيت أجهزة استشعار دفاعية في جميع أنحاء البلاد، في نظام أطلق عليه اسم أينشتاين، في دلالة على العبقرية، لردع أعداء أميركا.

لكن حسب رأي الصحيفة فإن هجوم التجسس الروسي الواسع على الحكومة الأميركية والشركات الخاصة الذي بدأ منذ الربيع واكتشفه القطاع الخاص قبل بضعة أسابيع، يعدّ من أكبر الإخفاقات الاستخباراتية في العصر الحديث.