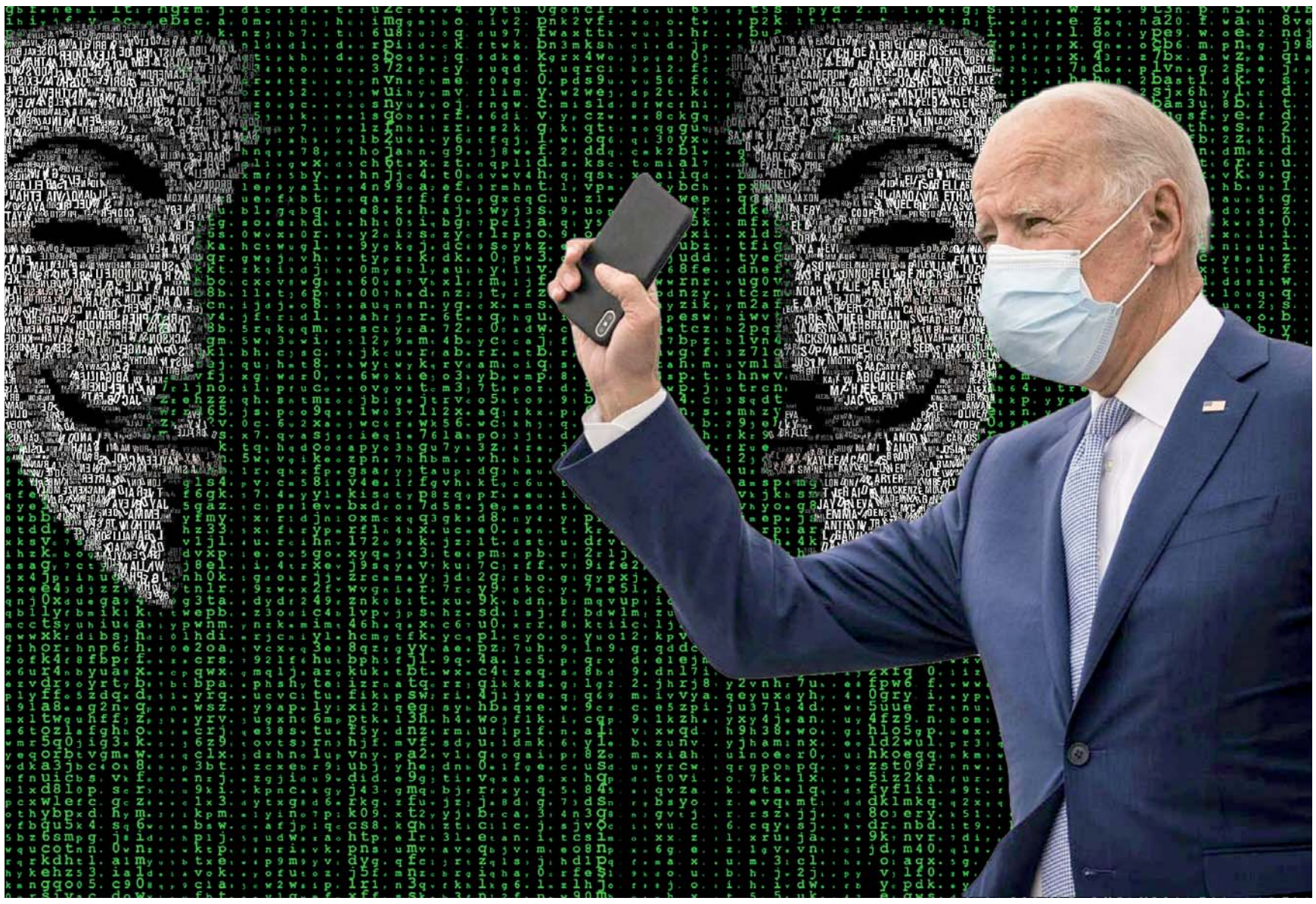
العرب
الأحد 2021/01/03
السنة 43 العدد 11929

الهجوم الإلكتروني الكبير.. يربك واشنطن ويختبر بايدن

القراصنة اخترقوا المنظومات الأميركية أبكر كثيرا مما يُعتقد

أحدث الاختراق الإلكتروني الكبير لمؤسسات ووكالات حكومية في الولايات المتحدة إرباكا بعد اكتشاف أن الهجوم كان منذ أشهر طويلة، وكان بمثابة ناقوس خطر لتعزيز أنظمة الدفاعات الإلكترونية، ووضع تحديات كبيرة مبكرة أمام الرئيس الأميركي الجديد جو بايدن بخصوص ردع الجهات المنفذة للهجوم ووضع خطط لتقوية الأمن السيبراني وتعزيزه في أكبر بلد في العالم.



الاختبار الصعب

واشنطن – سيكون الرئيس الجديد للولايات المتحدة جو بايدن أمام تحديات كبيرة بخصوص الأمن السيبراني ومكافحة عمليات القرصنة بعد الهجوم الإلكتروني الكبير الذي تعرضت له مؤسسات ووكالات حكومية أميركية حساسة على يد قراصنة يعتقد أنهم من روسيا.

وأظهر الهجوم الإلكتروني مدى الضعف الكبير الذي تعاني منه مؤسسات الولايات المتحدة على مستوى الأمن الإلكتروني، حيث أظهرت المعلومات الأولية أن عملية الاختراق كانت منذ أشهر طويلة ولم تكن منذ أوائل ديسمبر الماضي.

وفتحت عمليات التجسس واسعة النطاق والقرصنة باب الاتهامات بالتقاعس لإدارة الرئيس المنتهية ولايته دونالد ترامب بعد رفضه اتهام روسيا بالوقوف وراء الهجوم الإلكتروني الأكبر في تاريخ الولايات المتحدة والتقليل من حجم الاختراق، على الرغم من أن وزير خارجيته مايك بومبيو اتهم علانية وبوضوح موسكو بالمسؤولية عن هذا الهجوم.

وتقول وكالة الأمن الإلكتروني في الولايات المتحدة إن الوكالات الحكومية وكيانات البنية التحتية الحيوية ومؤسسات القطاع الخاص استهدفت من جانب من وصفتها بـ"جهة فاعلة متقدمة وخطرة" منذ مارس 2020 على الأقل. وهناك جهات حكومية أخرى تقول إن العبث ببرمجيات شركة "سولار ويندز" بدأ منذ أكتوبر 2019.

وزرع متسللون برنامجا خبيثا في شبكة تابعة لشركة البرمجيات "سولار ويندز" (SolarWinds) ضمن عملية مخابراتية اخترقت قلب الحكومة ومؤسسات عديدة في الولايات المتحدة ومؤسسات أخرى في مختلف أنحاء العالم، ولم يعرف حتى اللحظة حجم الأضرار، التي خلفها المتسللون قبل اكتشاف أمرهم في الثالث عشر من ديسمبر الماضي.

وسيدفع الاختراق الإلكتروني الكبير بايدن، بعد تسلم مهامه في العشرين من يناير الجاري، إلى تعزيز الموارد الإلكترونية لواشنطن على مستوى قدراتها الهجومية من أجل ممارسة سياسة ردع أفضل ضد الهجمات الإلكترونية المستقبلية من قبل روسيا وجهات دولية فاعلة أخرى.

ويتوقع مركز "ستراتفور" الأميركي للدراسات الإستراتيجية والأمنية أن يؤدي حجم اختراق "سولار ويندز" وتحفظ ترامب على إلقاء المسؤولية على عاتق روسيا إلى دفع بايدن إلى التصرف بوتيرة أسرع عند توليه منصبه.

ويقول خبراء المركز الأميركي إنه من المرجح أن تعمل الدولة على المزيد من الاستثمارات الأميركية في الدفاع السيبراني خلال السنوات الأربع المقبلة، إضافة إلى عمل إدارة بايدن على الاستمرار في فرض عقوبات على الدول المهاجمة.

وكشف الاختراق الإلكتروني عن ضعف الولايات المتحدة أمام عمليات اختراق أكبر وأوسع، وسلط الهجوم المشتبه به المرتبط بروسيا الضوء على تصعيد الأنشطة الإلكترونية التي ترعاها روسيا ضد المصالح الأميركية.

واستهدف الهجوم وكالات حكومية اتحادية أميركية من بينها إدارة الأمن النووي ووزارات الأمن الداخلي والخارجية والدفاع والطاقة والتجارة والخزانة، إضافة إلى مؤسسات خاصة عدة. وقالت شركة مايكروسوفت إن المتسللين تمكنوا من اختراقها والوصول إلى بعض شفرات المصادر.

واستغل القراصنة نظم برمجيات المراقبة الخاصة بشركة "سولار ويندز" المتمركزة في تكساس كأداة للوصول إلى شبكات حكومية حساسة وشركات تكنولوجيا أخرى.

الرد المنتظر

لم يتوان بايدن عن التهديد بجعل المسؤولين عن الهجوم الإلكتروني واسع النطاق يدفعون "ثمنا باهظا" عن فعلتهم. لكن، ينتظر معرفة طبيعة القرارات التي ستتخذها إدارته الجديدة بخصوص الرد على الاختراق الكبير.

ويرى مركز "ستراتفور" أن إدارة الرئيس الأميركي الجديد ستعمل على فرض عقوبات على كيانات وأفراد روس متورطين في التخطيط للهجوم وتنفيذه "إذا أمكن التعرف عليهم وربطهم به".

وتنفي روسيا بشدة مسؤوليتها عن الهجوم الإلكتروني الأكبر على مؤسسات أميركية حساسة، وعرضت على الولايات المتحدة التعاون الثنائي لمواجهة القرصنة الإلكترونية.

ويرجح المركز الأميركي أن يكون بايدن "أكثر عدوانية في لوم روسيا علانية" على الهجمات الإلكترونية وسيكون رده أسرع، ويشير إلى أن إدارة الرئيس الأميركي الجديد قد تقوم بإجراء هجوم إلكتروني انتقامي ضد روسيا باعتباره خيارا إضافيا إلى جانب العقوبات.

وكان الرئيس الأميركي المنتهية ولايته قد وقع على عدة جولات من العقوبات والهجمات الإلكترونية ضد روسيا ردا على هجمات إلكترونية شنت خلال ولايته.

ويتوقع أيضا أن تنحو الإدارة الأميركية الجديدة نفس المنحى الذي قام به ترامب ضد روسيا، خاصة بشأن فرض عقوبات، لكن مثل هذه العقوبات قد تكون ضيقة النطاق خوفا من تأجيج إجراءات انتقامية عدوانية ضد الكيانات الأميركية، والتسبب في إحداث أضرار اقتصادية كبيرة لدول مثل روسيا والصين التي تعتبر ضرورية للاقتصاد الدولي.

ويقول مركز "ستراتفور" إن بايدن سيعمل على مراجعة القدرات المؤسسية الفيدرالية بحثا عن طرق لزيادة القدرات الإلكترونية الدفاعية، فضلا عن التنسيق بين الوكالات المختلفة.

> الاختراق الإلكتروني يكشف ضعف الولايات المتحدة أمام عمليات أكبر وأوسع، ويسلط الضوء على الأنشطة التي تستهدف المصالح الأميركية

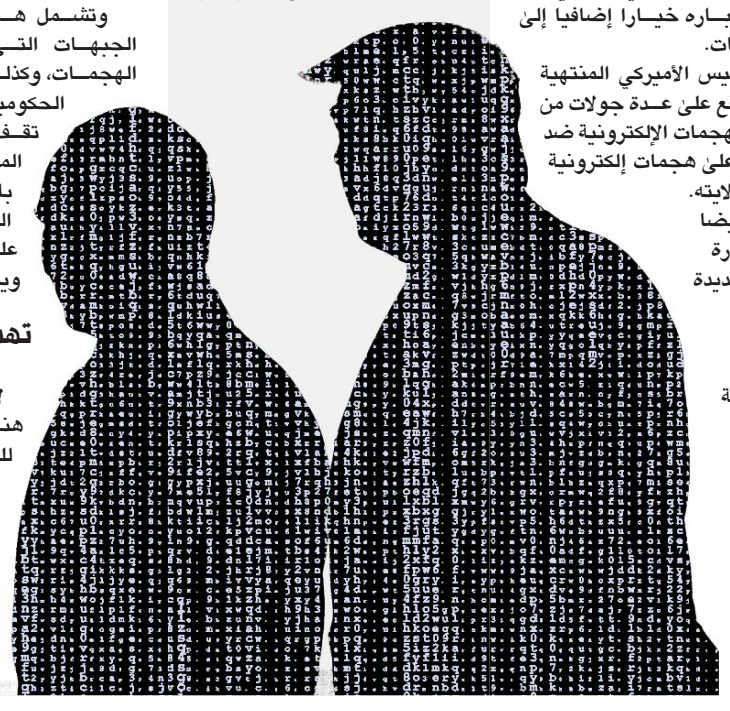
كما يتوقع مراجعة العمليات السيبرانية الهجومية والإستراتيجية العدوانية لبناء سياسة الردع، ويرى المركز الأميركي للدراسات الإستراتيجية والأمنية أن الإصلاح الجوهري المحيط بالطريقة التي تتعامل بها الولايات المتحدة مع الأمن السيبراني على غرار ذلك في أعقاب أحداث 11 سبتمبر 2001 غير مرجح ضمن عمليات المراجعة.

ويؤكد خبراء "ستراتفور" أن هجوم "سولار ويندز" كان بمثابة ناقوس خطر لتعزيز أنظمة الدفاعات الإلكترونية، الذي لا يبدو أنه كان له تأثير كاف يستلزم مثل هذه الإصلاحات.

وعوضا عن إجراء إصلاحات داخلية، سيكون سلاح العقوبات الأداة الأقرب بيد بايدن لاستخدامها للرد الدبلوماسي ضد المسؤولين عن عمليات الاختراق الإلكتروني.

ويتمتع الكونغرس الأميركي والرؤساء السابقون بتاريخ طويل في استخدام حظر السفر والطرد الدبلوماسي وتجميد الأصول وأشكال أخرى من العقوبات ضد المتسللين الروس والإيرانيين والكوريين الشماليين والصينيين، الذين ينفذون هجمات إلكترونية ضد الولايات المتحدة.

وتشمل هذه الإجراءات عادة الجهات التي تُستخدم لتنفيذ الهجمات، وكذلك الأفراد والهيئات الحكومية المحددة التي تقف وراء الهجمات. ومن المرجح أن تستمر إدارة بايدن في مثل هذه الممارسات، بدءًا بالرد على هجوم "سولار ويندز".



تهديدات متزايدة

لا يتوقع أن تكون هناك تأثيرات مباشرة للعقوبات على الجهات المنفذة للهجمات الإلكترونية واسعة النطاق، حيث يرى مركز "ستراتفور" أن "التطور السريع للقدرات الإلكترونية جنبا إلى جنب مع إحجام واشنطن عن قبول الضرر الاقتصادي والسياسي المصاحب للعقوبات الصارمة إلى الحد من خيارات سياسة بايدن لتقويض التهديدات الإلكترونية".

ويمتلك العديد من الأفراد والكيانات المتورطة في تنفيذ الهجمات أصولاً محدودة في الولايات المتحدة والغرب عموما، مما يجعل تأثير العقوبات المالية ضئيلا بشكل نسبي. ومن أجل إحداث ضرر اقتصادي مباشر، ستحتاج العقوبات الأميركية إلى استهداف الاقتصاد الأوسع للدولة المهاجمة مثل تلك التي فرضتها إدارة ترامب على صادرات النفط الإيرانية.

ويقول خبراء "ستراتفور" إنه عادة ما تقتصر العقوبات على الدول التي تعتبرها الولايات المتحدة مارقة مثل إيران وفنزويلا وكوبا وكوريا الشمالية. وإن فرض عقوبات شاملة على الصين، الشريك التجاري الأكبر للولايات المتحدة ستكون له تداعيات كارثية على الاقتصاد الأميركي، كما أن مثل هذه العقوبات على روسيا ستكون لها تداعيات سياسية شديدة بالمثل على السياسة الخارجية الأميركية.

ويرى هؤلاء أن سياسة ردع العمليات الإلكترونية الأميركية عززت استعداد الدول الأخرى لشن هجمات ضد الولايات المتحدة. وبالنسبة إلى الصين، على وجه الخصوص، فإن الإستراتيجية الاقتصادية لواشنطن التي منعت الصين من الوصول إلى التكنولوجيا الأميركية قد زادت من حاجة بكين إلى تنفيذ هجمات إلكترونية تتعلق بالتجسس الصناعي.

كما أن الولايات المتحدة مقيدة بدرجة أكبر في أنواع النشاط السيبراني التي ترغب في القيام به بسبب المعايير القانونية في الداخل ورد الفعل السلبي المحلي المحتمل إذا أثار هذا النشاط رد فعل سلبي من قبل روسيا أو الصين. وهذا يقلل من قدرة الولايات المتحدة على تحمل المخاطر في أي هجمات يمكن أن تهدف إلى تعزيز سياسة الردع.

وضمن هذا الوضع العام، فإنه يتوقع أن تعمل روسيا والصين على زيادة استخدام استراتيجيات الهجمات الإلكترونية للوصول إلى المعلومات الاستخباراتية وإجراء التجسس الصناعي بشكل متزايد، في حال فشلت عمليات ردع أو منع التهديدات السيبرانية المستقبلية.

ويقول مركز "ستراتفور" إن "سرقة الأسرار التجارية من خلال الوسائل الإلكترونية ستصبح بدورها تهديدا متزايدا، لاسيما من الصين"، خاصة في حال عدم قدرة الولايات المتحدة على ردع الهجمات الإلكترونية المدعومة من الدول المهاجمة.

ويرى المركز أن فشل الردع سيؤدي إلى زيادة تكاليف التخفيف من حدة الهجمات الإلكترونية والتعامل معها، وهو ما يتوقع أن يزيد الضغط العالمي من أجل الإجماع متعدد الأطراف لمعالجة مثل هذه الأنشطة.

Stratfor | WORLDVIEW™

مركز «ستراتفور» الأميركي للدراسات الإستراتيجية والأمنية:

بايدن سيكون أكثر عدوانية في لوم روسيا على الهجمات الإلكترونية

وتقول شركة "سايبر سيكيوريتي فنتشرو"، المختصة في الجرائم الإلكترونية في تقرير صدر في نوفمبر الماضي، إن التكلفة السنوية التي يتحملها الاقتصاد العالمي لجميع الجرائم الإلكترونية بما في ذلك النشاط السيبراني المدعوم من الدول المهاجمة ستنمو بنسبة 15 في المئة سنويا على مدى السنوات الخمس المقبلة لتصل إلى 10.5 تريليون دولار بحلول عام 2025.

ويحتم استمرار الانتشار المتزايد للهجمات الإلكترونية والزيادة في عدد الدول القادرة على تنفيذها في دفع الولايات المتحدة وروسيا وأوروبا والصين إلى وضع معايير تحكم المجال السيبراني العالمي.

ومن شأن هذه المعايير أن تحد من مخاطر التصعيد من خلال التحديد الواضح للأنواع المختلفة للنشاط السيبراني، وما يمكن اعتباره استجابة مناسبة لكل منها، إلا أن الجهود السابقة للتفاوض بشأن معايير الأمن السيبراني العالمية فشلت في الحصول على دعم الولايات المتحدة وروسيا وأوروبا والصين أكبر اقتصادات وجهات فاعلة عبر الإنترنت.