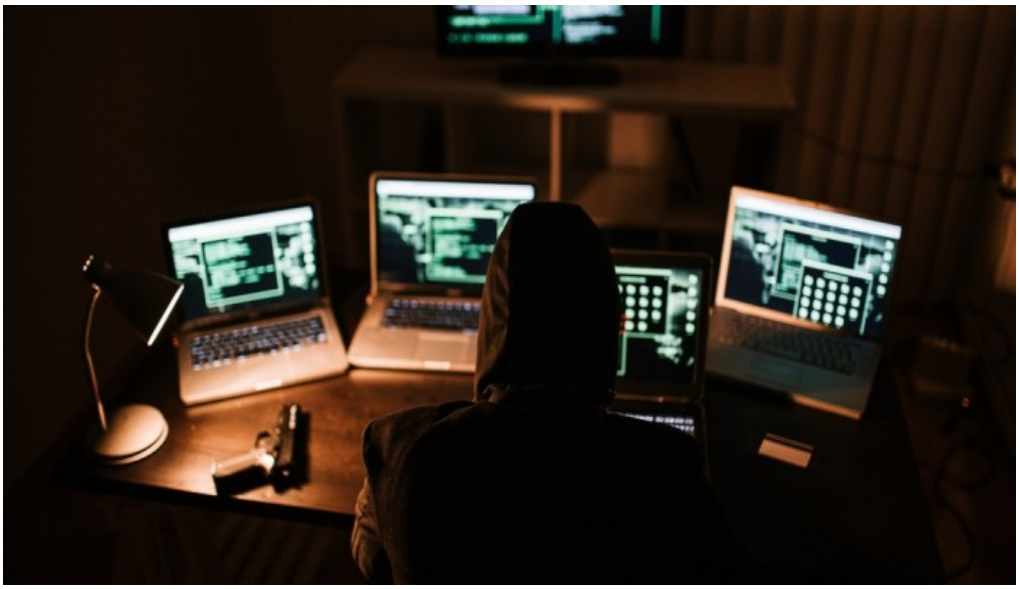
هل تشن روسيا هجمات إليكترونية على أمريكا؟



الخميس 24 مارس 2022 12:23 م

مع ارتفاع حدة التوترات في المواجهة بشأن أوكرانيا، حذرت وزارة الأمن الداخلي الأمريكية، من أن رد الولايات المتحدة على غزو روسي محتمل قد يؤدي إلى هجوم إلكتروني تشنه الحكومة الروسية أو وكلائها ضد الولايات المتحدة.

وقال الرئيس الأمريكي، جو بايدن، إن المعلومات الاستخباراتية تؤكد ذلك، وأن الولايات المتحدة تعتقد أن "الحكومة الروسية تبحث خيارات"، مضيفًا أن روسيا "تبحث" تنفيذ هجوم إلكتروني ضد الولايات المتحدة، لكن واشنطن سوف تستخدم "كل أداة" لمنع مثل ذلك التحرك والرد عليه، وفقًا لـ"BBC".

لماذا؟

كان وزير الخارجية الروسي سيرغي لافروف قال قبل أيام إن العلاقات بين موسكو وواشنطن أصبحت على "حافة الانهيار".

ويرى بايدن أن موسكو يمكنها تنفيذ هذه الهجمات من باب التصعيد، بعد العقوبات التي فُرضت عليها عقب غزو أوكرانيا، أو قد يكون مدفوعا بـ"الكلفة الاقتصادية غير المسبوقة" التي تتكبدها روسيا خلال الأيام السابقة.

وخاطب بايدن الشركات الأمريكية بأن "تسرّع وتيرة الجهود التي تبذلها في سبيل إحكام أبوابها الرقمية"، مضيفًا "لديكم القوة والقدرة والمسؤولية لتعزيز الأمن الإلكتروني والمتانة فيما يتعلق بالخدمات والتكنولوجيا الحيوية التي يعتمد عليها الأمريكيون. نريد من الجميع أداء أدوارهم".

المخاطر

وتحذر الولايات المتحدة وبريطانيا مما يسمى بـ"الامتداد"، وهو الذي تُستهدف فيه دول أخرى أو يخرج فيه هجوم من مسرح الصراع عن طريق الخطأ.

والمثال الذي تردده السلطات يتمثل في هجوم مسح إلكتروني (NotPetya wiper)، الذي شنه قراصنة تابعون للجيش الروسي، وانتشرت تلك البرمجية الخبيثة بشكل خارج عن السيطرة في عام 2017، ما أدى إلى انهيار آلاف الشركات في شتى أنحاء العالم، وتسبب في أضرار تقدر بنحو 10 مليارات دولار.

وربما يتعلق الخوف من ضرب البنية التحتية الأمريكية، مثل ما حدث العام الماضي في منطقة الساحل الشرقي عندما تسبب قراصنة في قطع إمدادات خط أنابيب للنفط.

وفي أسوأ السيناريوهات، قد يؤدي هجوم إلكتروني كبير على الولايات المتحدة أو عضو آخر في الناتو إلى تفعيل البند 5، المتعلق بالدفاع الجماعي.

أمريكا مهددة

ونشأ نصف الهجمات الإلكترونية في العام الماضي من روسيا، وفقًا لتقرير الدفاع الرقمي السنوي للشركة، 52 في المئة من محاولات القرصنة التي ترعاها الدولة من يوليو 2019 ويونيو 2020 كانت روسية الأصل، وفقًا لتقارير شركة مايكروسوفت.

بينما 25% خلال هذه الفترة الزمنية من إيران، و12% من الصين و11% المتبقية من كوريا الشمالية ودول أخرى.

وتحملت الولايات المتحدة العبء الأكبر من الهجمات الإلكترونية في العام الماضي، تليها المملكة المتحدة، بينما أكثر من ثلثي إلى 69% - من إشعارات NSN المرسلة من قبل Microsoft من يوليو 2019 إلى يونيو 2020 كانت إلى عملاء في الولايات المتحدة.

كما تم إرسال 19% من الهجمات الإلكترونية في العام الماضي إلى عملاء في المملكة المتحدة، تليها 5 % في كندا، و4% في كوريا الجنوبية و3% في المملكة العربية السعودية، بحسب تقرير مايكروسوفت.

أما إيران - تمثل ثاني أكبر عدد من محاولات الاختراق بعد روسيا – فقد كانت مصدرًا لزيادة النشاط السيبراني المدعوم من الدولة، ففي فترة 30 يومًا بين أغسطس وسبتمبر 2019، لاحظت Microsoft أن متسللين مقرهم إيران يهاجمون 241 حسابا لعملاء الشركة.

سوابق روسيا

وبدأت الهجمات الروسية على أمريكا في عام 1996 بهجوم Moonlight Maze، وهي واحدة من أولى حملات التجسس السيبراني التي ترعاها موسكو، وفقًا لـ"فوربس".

حينها تم إلقاء اللوم على روسيا في هجمات Moonlight Maze، والتي تضمنت سرقة كمية هائلة من المعلومات السرية من العديد من الوكالات الحكومية بما في ذلك وزارة الطاقة ووكالة ناسا ووزارة الدفاع الأمريكية.

وفي عام 2008، بدأت مجموعة قرصنة روسية تُدعى تورلا، بمهاجمة الأنظمة العسكرية الأمريكية باستخدام الخداع والأبواب الخلفية والجذور الخفية وإصابة المواقع الحكومية
في حينها أيضا، تم إلقاء اللوم على المخابرات الروسية في الهجوم؛ بينما في عام 2017، تمكن أربعة باحثين كمبيوتر من Kaspersky Labs وKings Collegeg في لندن من الحصول على خادم الطرف الثالث المستخدم لتوجيه هجمات Moonlight Maze؛ وأظهرت النتائج أن روسيا هي وراء ذلك
وقبل عدة سنوات، قامت مجموعة قرصنة روسية أخرى تعرف باسم APT-28، باختراق اللجنة الوطنية الديمقراطية، وكذلك البيت الأبيض والبرلمانين الألماني والنرويجي، ومنظمة الأمن والتعاون في أوروبا، والصحفيين