واشنطن تدخل في مواجهة مع المجرمين الإلكترونيين

التهديد بتدمير البنية التحتية لفارضي الفدية الإلكترونية المتسللين عبر الثغرات الأمنية

أثارت الهجمات الإلكترونية التي استهدفت شركات عالمية ومنشآت أميركية قلقا أمنيا كبيرا نظرا لإضرار هجمات الفدية الإلكترونية بمصالح حساسة مثل ملفات الشرطة، فضلا عن تهديد سلاسل الغذاء العالمية عبر ضرب كبار الشركات المتخصصة في مجال بيع اللحوم في وقت تعد فيه واشنطن بتدمير البنية التحتية لفارضي الفدية.

التراشق بالتهم سيد الموقف

واشنطن – تسبب المجرمون الإلكترونيون الأجانب في شلل المدارس والمستشفيات الأميركية وتسريب ملفات الشرطة الحساسة ونقص الوقود، ويهددون اليوم سلاسل الإمداد الغذائي العالمية.

وتقوم برامج الفدية بإغلاق وصول الضحايا إلى معلوماتهم وتشفيرها حيث لا يمكن تجاوزها إلا من خلال دفع الضحية لفدية.

وقال وزير الخارجية الأميركي أنتوني بلينكن الاثنين إن واشنطن تعمل على تطوير استراتيجية لمكافحة طلب فدية وحماية شبكة الإنترنت بشكل أفضل "لتدمير البنى التحتية لفارضي الفدية وجلبهم إلى العدالة".

وتأتي تصريحات وزير الخارجية بعد يومين من تحذير وزيرة التجارة الأميركية جينا ريموندو من "التهديد الدائم" الذي تشكله الجرائم الإلكترونية التي "يمكن أن تتزايد"، وقالت إنه يجب أن نفترض أن "هذه الهجمات ستبقى موجودة إلى الأبد".

وأكد بلينكن أن العمل يجري بالتعاون مع القطاع الخاص "لإيجاد المنخرطين بهذه الأعمال ومنع الدول التي تستضيفهم من القيام بذلك".

ويعتبر العديد من الخبراء أن قراصنة المعلوماتية الذين يقفون وراء هذه الهجمات موجودون في روسيا.

وأعلنت وزارة العدل الأميركية الاثنين أنها استعادت عملة مشفرة بقيمة 2.3 مليون دولار من هجوم برنامج الفدية الذي تعرضت له شركة "كولونيال بايبلاين" الشهر الماضي، والذي نجم عنه انقطاع لمدة ستة أيام في نظام خطوط الأنابيب النفطية.


أندري نوغييرا

دفع الفدية المالية كان قرارا مؤلما للغاية، لشركتنا

وبهذا، استعادت الحكومة الأميركية أكثر من نصف قيمة الفدية المالية البالغة 4.4 مليون دولار والتي سدّدتها شركة كولونيال بايبلاين لمجموعة القرصنة.

وتعرضت شركات أميركية أو أخرى تعمل في الولايات المتحدة في الآونة الأخيرة لعدة هجمات معلوماتية واسعة النطاق أدت الى إبطاء أو حتى وقف إنتاجها.

وبعد أن هوجمت شركة الأنابيب، هاجم قراصنة شركة لإنتاج اللحوم مقرها في الولايات المتحدة، كما أنه يبدو أيضا أنهم يخططون لمهاجمة محطات تلفزيون ووسائل إعلام.

وتوقفت ثلاث محطات إخبارية تلفزيونية على الأقل عن العمل تماما الخميس الماضي، فيما يعتقد خبراء أنه أحدث هجمات "الفدية" التي يستغل منفذوها ثغرات أمنية لتعطيل أنظمة معلوماتية والمطالبة لاحقا بفدية من أجل إعادة تشغيلها، وفقا لما نقلته شبكة "أن. بي.سي نيوز" الأميركية.

وتسبب الهجمات بإجبار الموظفين على إغلاق أجهزة الكمبيوتر والهواتف الخاصة بالشركة.

وتعرضت شركة "جي.بي.إس" البرازيلية، وهي الأكبر في مجال معالجة اللحوم في العالم، لهجوم إلكتروني تسبب في توقف مؤقت لبعض عملياتها في الولايات المتحدة وكندا وأستراليا.

واخترقت شبكات الكمبيوتر الرئيسية للشركة، وهو ما أثر على الآلاف من العمال.

وقال البيت الأبيض إن الشركة تعتقد أن هجوما نفذته جماعة إجرامية، مقرها روسيا على الأرجح، بغرض طلب فدية.

وأعلنت مجموعة الأغذية الزراعية البرازيلية العملاقة "جي.بي.أس"، أضخم شركة في العالم في مجال تعبئة اللّحوم، الأربعاء أنّها دفعت فدية مالية قدرها 11 مليون دولار بعملة البيتكوين لقراصنة معلوماتية هاجموها.

وقال أندري نوغييرا الرئيس التنفيذي للفرع الأميركي للمجموعة في بيان إنّ دفع الفدية المالية "كان قرارا مؤلما للغاية لشركتنا ولي أنا شخصيا".

وأضاف "لكنّنا شعرنا بضرورة اتخاذ هذا القرار لمنع أيّ مخاطر محتملة على زبائننا".

وأوضح البيان أنّ الشركة دفعت "ما قيمته 11 مليون دولار فدية ردًا على القرصنة الإجرامية لعملياتها".

وفي مقابلة مع صحيفة "وول ستريت جورنال" قال نوغييرا إنّ الفدية المالية دُفعت بعملة البيتكوين الرقمية المشفّرة.

ولفت البيان إلى أنّ "وقت الدفع، كانت الغالبية العظمى من مرافق الشركة تعمل"، مشيرا إلى أنّ المجموعة قرّرت دفع الفدية "لضمان عدم تسرّب أيّ بيانات" و"تجنّب أيّ مشاكل غير متوقّعة مرتبطة بالهجوم".

وكان الفرع الأميركي للمجموعة البرازيلية أخطر السلطات الأميركية بأنه تعرّض لهجوم إلكتروني باستخدام برنامج فدية مصدره "منظمة إجرامية مقرّها على الأرجح في روسيا"، وفقا للبيت الأبيض.

وعقب هذا الهجوم قال الرئيس الأميركي جو بايدن إنّه لا يستبعد اتخاذ إجراءات انتقامية ضدّ روسيا.

واستهدف الهجوم السيبراني خوادم تعتمد عليها الأنظمة المعلوماتية للمجموعة في أميركا الشمالية وأستراليا، وقد أدّى بالخصوص إلى شلّ أنشطة المجموعة في أستراليا وتعليق بعض خطوط الإنتاج في الولايات المتحدة.

و"جي.بي.إس" هي شركة متخصّصة في منتجات لحوم البقر والدجاج والخنازير، وهي إحدى أضخم شركات المواد الغذائية في العالم.

وإلى جانب البرازيل وسائر دول أميركا اللاتينية، لهذه الشركة وجود في كلّ من الولايات المتّحدة وكندا وأستراليا ونيوزيلندا وبريطانيا.

وغالبا ما تستهدف هجمات إلكترونية مماثلة الشركات المتعدّدة الجنسيات حول العالم.

وفي مطلع مايو استهدف هجوم سيبراني شركة "كولونيال بايبلاين" التي تمتلك أكبر شبكة لأنابيب الوقود في الولايات المتحدة ترسل البنزين ووقود الطائرات من ساحل خليج تكساس إلى الساحل الشرقي المكتظ بالسكّان.

ولاحقا أقرّت الشركة بأنّها دفعت للقراصنة فدية بعملة البيتكوين قدرها 4.4 مليون دولار.

والإثنين أعلنت وزارة العدل الأميركية أنّها استعادت أكثر من نصف قيمة هذه الفدية من مجموعة القرصنة الإلكترونية "داركسايد" التي نفذت الهجوم السيبراني على "كولونيال بايبلاين".

ويثير الخراب الذي تسببه عصابات برامج الفدية سؤالا واضحا: لماذا بدت الولايات المتحدة، التي يُعتقد أنها تمتلك أعظم القدرات الإلكترونية في العالم، عاجزة جدا عن حماية مواطنيها من هذا النوع من المجرمين الذين يعملون بإفلات شبه كامل من العقاب من روسيا والدول الحليفة؟

ويكمن الجواب بأن هناك العديد من العقبات التكنولوجية والقانونية والدبلوماسية التي تحول دون ملاحقة عصابات برامج الفدية. فحتى وقت قريب، لم تكن هذه القضية أولوية عالية للحكومة الأميركية.

لكن ذلك تغير لأن المشكلة نمت إلى ما بعد مجرد إزعاج اقتصادي. ويعتزم الرئيس بايدن مواجهة نظيره الروسي فلاديمير بوتين بشأن إيواء موسكو لمجرمي برامج الفدية الإلكترونية عندما يلتقي الرجلان في أوروبا في وقت لاحق من هذا الشهر. كما وعدت إدارة بايدن بتعزيز الدفاعات ضد الهجمات، وتحسين الجهود لمحاكمة المسؤولين وبناء تحالفات دبلوماسية للضغط على الدول التي تؤوي عصابات برامج الفدية.

تطويق حركة فارضي الفدية

تتزايد الدعوات للإدارة لتوجيه وكالات الاستخبارات الأميركية والجيش لمهاجمة البنية التحتية التقنية لعصابات برامج الفدية المستخدمة في قرصنة بيانات الضحية الحساسة ونشرها على شبكة الإنترنت المظلمة وتخزين مدفوعات العملة الرقمية.

وقال جون ريجي، العميل السابق في مكتب التحقيقات الفدرالي وكبير مستشاري الأمن السيبراني والمخاطر لجمعية المستشفيات الأميركية، إن محاربة برامج الفدية تتطلب مكافئا غير قاتل لـ"الحرب العالمية على الإرهاب" التي بدأت بعد هجمات 11 سبتمبر. فقد تضرر الكثيرون بشدة من عصابات برامج الفدية خلال جائحة فايروس كورونا.

وتابع ريجي "يجب أن يشمل النهج المُتّبع مزيجا من العمليات الدبلوماسية والمالية وعمليات إنفاذ القانون والاستخبارات والعمليات العسكرية".

وقدمت فرقة عمل عامة وخاصة، بما في ذلك مايكروسوفت وأمازون، اقتراحات مماثلة في تقرير من 81 صفحة دعا وكالات الاستخبارات والقيادة الإلكترونية الأميركية التابعة للبنتاغون إلى العمل مع الوكالات الأخرى "لإعطاء الأولوية لعمليات تعطيل برامج الفدية".

وقال المؤلف الرئيسي للتقرير فيليب راينر، الذي عمل في مجلس الأمن القومي خلال رئاسة أوباما وهو الآن الرئيس التنفيذي في معهد الأمن والتكنولوجيا "استهدف بنيتهم التحتية، وطارد مَحافظهم، وقدرتهم على صرف المال".

لكن الصعوبات في القضاء على عصابات برامج الفدية ومجرمي الإنترنت الآخرين كانت واضحة منذ فترة طويلة. فقد نمت قائمة مكتب التحقيقات الفدرالي لأهم المجرمين السيبرانيين المطلوبين بسرعة كبيرة ولديها الآن أكثر من 100 اسم، لا يخطئ كثير منهم. إذ أن أفغيني بوغاتشيف، الذي وجهت إليه لائحة اتهام منذ ما يقرب من عقد من الزمان لما وصفه المدعون بأنها موجة من سرقات البنوك الإلكترونية، يعيش في منتجع روسي و"معروف بأنه يستمتع بركوب القوارب" على البحر الأسود، وفقا لإدراج مكتب التحقيقات الفدرالي.

ويمكن لعصابات برامج الفدية التحرك، ولا تحتاج إلى الكثير من البنية التحتية للعمل ويمكنها حماية هويات أفرادها. كما أنها تعمل في شبكة لامركزية. على سبيل المثال، تؤجّر دارك سايد، المجموعة المسؤولة عن هجوم خط الأنابيب الذي أدى إلى نقص الوقود في الجنوب، برنامج الفدية الخاص بها للشركاء لتنفيذ الهجمات.

وقالت كاتي نيكلز مديرة الاستخبارات في شركة الأمن الإلكتروني رید کاناري، إن تحديد مجرمي برامج الفدية وتعطيلهم يستغرق وقتا وجهدا جادا.

وتابعت "يسيء كثير من الناس فهم أن الحكومة لا يمكنها فقط الضغط على زر والقول، حسنا، دمّر هذا الكمبيوتر... ليست المهمة سهلة، حتى بالنسبة إلى مجتمعات الاستخبارات".

وقال راينر إن هذه القيود لا تعني أن الولايات المتحدة لا تزال غير قادرة على إحراز تقدم في هزيمة برامج الفدية، وقارن الوضع بقدرة الولايات المتحدة على إضعاف جماعة القاعدة الإرهابية بينما لم تعتقل زعيمها أيمن الظواهري، الذي تولى السلطة بعد أن قتلت القوات الأميركية سلفه أسامة بن لادن.

وتابع راينر "يمكننا بسهولة أن نقول إن القاعدة لم تعد تشكل تهديدا للوطن. إذا لم تنل من الظواهري، فإنك تدمر قدرته على العمل في الواقع. هذا ما يمكنك فعله لهؤلاء الرجال (الذين يديرون برامج الفدية)".

البنتاغون على الخط

كان البيت الأبيض غامضا بشأن ما إذا كان يخطط لاستخدام تدابير إلكترونية هجومية ضد عصابات برامج الفدية. وقالت السكرتيرة الصحافية جينيفر بساكي الأربعاء "لن نستبعد الخيارات من على الطاولة"، لكنها لم تخض في التفاصيل. وجاءت تعليقاتها بعد هجوم فدية نظّمته عصابة روسية وتسبب في انقطاع الخدمة في شركة فريبوي (جي. بي.إس) البرازيلية، ثاني أكبر منتج للحوم البقر ولحم الخنزير والدجاج في الولايات المتحدة.

وقال الجنرال بول ناكاسوني، الذي يقود القيادة الإلكترونية الأميركية ووكالة الأمن القومي، خلال ندوة عقدت مؤخرا إنه يعتقد أن الولايات المتحدة ستعمل على القضاء على برامج الفدية، بخطط ستشمل وزارة الدفاع.

وقال السناتور أنغوس كينج، وهو مستقل عن ولاية ماين وزعيم تشريعي بشأن قضايا الأمن السيبراني، إن النقاش في الكونغرس حول مدى قوة الولايات المتحدة التي يجب أن تكون ضد عصابات الفدية، وكذلك خصوم الدولة، سيكون الأهم خلال الأشهر القادمة.

وأشار إلى أن الأمر معقد لأنك تتحدث عن استخدام الوكالات الحكومية وقدراتها لملاحقة المواطنين العاديين في بلد آخر.

ويُعتقد على نطاق واسع أن الولايات المتحدة تمتلك أفضل القدرات الإلكترونية الهجومية في العالم، على الرغم من أن التفاصيل حول مثل هذه الأنشطة شديدة السرية شحيحة. وتُظهر الوثائق التي سربها المقاول السابق لوكالة الأمن القومي إدوارد سنودن أن الولايات المتحدة نفذت 231 عملية هجومية إلكترونية في 2011. وقبل أكثر من عقد من الزمان هاجم فايروس يسمى ستوكسنت وحدات تحكم لأجهزة الطرد المركزي في موقع تحت الأرض في إيران، مما تسبب في خروج الأجهزة الحساسة عن السيطرة وتدمير نفسها. ونُسب الهجوم الإلكتروني إلى الولايات المتحدة وإسرائيل.

> الهجوم على شركة «جي. بي.إس» البرازيلية، الأكبر في مجال معالجة اللحوم، تسبب في توقف مؤقت لبعض عملياتها في الولايات المتحدة وكندا وأستراليا

> 2.3 مليون دولار قيمة العملة الرقمية التي استعادتها وزارة العدل من الهجوم على كولونيال بايبلاين

وتسمح سياسة الولايات المتحدة المسماة "المشاركة المستمرة" بالفعل للمقاتلين الإلكترونيين بإشراك قراصنة معادين في الفضاء الإلكتروني وتعطيل عملياتهم باستخدام التعليمات البرمجية. وشنت القيادة الإلكترونية الأميركية عمليات هجومية تتعلق بأمن الانتخابات، بما في ذلك ضد مسؤولي المعلومات المضللة الروس خلال انتخابات التجديد النصفي الأميركية في 2018.

وبعد الهجوم على خط الأنابيب، وعد بايدن بأن إدارته ملتزمة بتقديم مجرمي الإنترنت الأجانب إلى العدالة. ومع ذلك، وحتى أثناء حديثه من البيت الأبيض، كانت عصابة فدية مختلفة مرتبطة بروسيا تتورّط في تسريب الآلاف من الملفات الداخلية الحساسة من قسم الشرطة في عاصمة البلاد. ويعتقد الخبراء أن هذا هو أسوأ هجوم من برمجيات الفدية ضد وكالة إنفاذ القانون في الولايات المتحدة.