نيويورك تايمز | نشر في ٧ أكتوبر ٢٠١٩,

مع تصاعد التهديدات لسنة 2020.. قراصنة إيرانيون يستهدفون حملة ترامب

ترجمة وتحرير: نون بوست

كتب: نيكول بيرلوث و ديفيد سانجر

أقرّ الباحثون الأمنيون ومسؤولو المخابرات بأنه بالإضافة إلى إيران، بدأ قراصنة من روسيا وكوريا الشمالية في استهداف المنظمات التي تعمل عن كثب مع مرشحي الرئاسة في الولايات المتحدة. وقال أورين فالكويتز، الرئيس التنفيذي لشركة آريا 1 للأمن السيبراني: "لقد شهدنا هجمات على العديد من الحملات الانتخابية ونعتقد أنه سيزداد حجمها وشدّتها مع اقتراب موعد الانتخابات".

في هذا الصدد، أكّدت أحدث تقارير مايكروسوفت أنّه من المرجّح أن تتسارع الهجمات الإلكترونية وحملات التشويه للمرشحين السياسيين بحلول سنة 2020. وفي سنة 2016، تسلل الروس إلى شبكات الكمبيوتر الخاصة بالديمقراطيين والجمهوريين ثم قاموا بنشر رسائل البريد الإلكتروني للديمقراطيين بشكل انتقائي بما في ذلك رسائل جون د. بوديستا، رئيس حملة هيلاري كلينتون، في محاولة لإلحاق الضرر بحملة السيدة كلينتون.

في سياق متّصل، أشارت مايكروسوفت إلى حدوث هجمات على مدار 30 يومًا بين آب/ أغسطس وأيلول/ سبتمبر، وذلك إثر إعلان إدارة ترامب عن فرض عقوبات إضافية على إيران بعد أكثر من عام على انسحاب الرئيس الأمريكي من الاتفاق النووي مع طهران سنة 2015. وأقر المسؤولون الإيرانيون بأن هذه العقوبات التي تهدف إلى تقليص عائدات إيران من النفط دفعت اقتصاد البلاد إلى الركود.

صرح مسؤولون من مكتب التحقيقات الفيدرالي ووزارة الأمن الداخلي ووكالة الأمن القومي طوال

أسابيع، بأنهم قلقون بشكل خاص بشأن الهجمات المدعومة من قبل إيران

في الآونة الأخيرة، نظرت الإدارة الأمريكية في إمكانية توجيه ضربة إلكترونية ضد طهران لمعاقبتها على الهجوم الذي استهدف منشآت نفط سعودية الشهر الماضي. وكلّ هذا يندرج ضمن النزاع السيبراني اليومي بين البلدين. وأضافت مايكروسوفت أن قراصنة إيرانيين شاركوا في حملة واسعة ضد المستهدفين في الولايات المتحدة. كما كشفت الشركة أن القراصنة حاولوا مهاجمة 241 حسابًا بالاعتماد على وسائل بسيطة إلى حد ما. ويبدو أن القراصنة استخدموا المعلومات المتاحة عن ضحاياهم عبر الإنترنت لاكتشاف كلمات المرور الخاصة بهم، ولكن لم يتضح بعد محتوى المعلومات التي سرقوها.

على الرغم من أن مايكروسوفت لم تذكر الأشخاص المستهدفين من قبل إيران، إلا أنها وجدت أدلة على أن القراصنة تسللوا إلى رسائل البريد الإلكتروني في أربع مناسبات على الأقل، لكن الاختراقات الناجحة لم تستهدف أيّة حملة رئاسية. حيال هذا الشأن، قال مدير الاتصالات في حملة ترامب الانتخابية تيم مورتو: "ليس لدينا أي مؤشر على استهداف أي من مكونات البنية التحتية الأساسية لحملتنا". كما أكد ممثلو مرشحين رئاسيين آخرين يوم الجمعة أن حملاتهم لم تكن مستهدفة.

علاوة على ذلك، صرح مسؤولون من مكتب التحقيقات الفيدرالي ووزارة الأمن الداخلي ووكالة الأمن القومي طوال أسابيع، بأنهم قلقون بشكل خاص بشأن الهجمات المدعومة من قبل إيران. يبدو أن مخاوفهم ناتجة عن تزايد التوترات بشأن العقوبات الجديدة على إيران وأنشطتها الناشئة خلال الانتخابات النصفية للعام 2018. وبينما يعتقد المسؤولون أن جميع الحملات الرئاسية شكلت أهدافًا محتملة، فإن حملة الرئيس ترامب اعتبرت منذ فترة طويلة الأكثر استهدافا.

الشي الوحيد الذي يعترف به المسؤولون الإيرانيون عند سؤالهم عن الهجمات الإلكترونية هو أنها ثنائية الاتجاه

في الواقع، كان الرئيس ترامب الطرف الذي تخلى عن الصفقة النووية وزاد في حدة العقوبات، كما صنفت الولايات المتحدة الحرس الثوري الإيراني مجموعة إرهابية. حسب بعض الروايات، يشرف فيلق الحرس الثوري على البرنامج النووي، بينما يعتبر الفيلق الإلكتروني الإيراني أفضل مجموعات الاختراق في إيران. في المقابل، ليس من الواضح ما إذا كانت المجموعة التي حددتها مايكروسوفت تنتمي إلى الفيلق الإلكتروني أم أنها تتكون عن قصد من العاملين للحساب الخاص وغيرهم ممن يصعب تتبع انتماءاتهم.

لكن الشي الوحيد الذي يعترف به المسؤولون الإيرانيون عند سؤالهم عن الهجمات الإلكترونية هو أنها ثنائية الاتجاه. وتجدر الإشارة إلى أن الولايات المتحدة استخدمت الأسلحة السيبرانية ضد أهداف إيرانية ثلاث مرات خلال العقد الماضي. وقد أدى الهجوم الأكثر شهرة، تحت الاسم الحركي "عملية الألعاب الأولمبية"، إلى تدمير حولي ألف جهاز طرد مركزي في موقع مجمع تخصيب اليورانيوم في نطنز.

في الأسابيع الأخيرة، طُلب من القيادة الإلكترونية الأمريكية وضع خيارات للرد على هجمات الصواريخ والطائرات من دون طيار التي استهدفت حقول النفط في المملكة العربية السعودية. وأفاد المسؤولون بأن أفضل خيار يتمثل في توجيه ضربة إلكترونية ضد إيران، في محاولة لتجنب التصعيد الذي قد تخلفه الضربات التقليدية. حتى الآن، لا يوجد دليل على اتخاذ هذا الإجراء نظرا لأن الوصول إلى شبكات الكمبيوتر الإيرانية قد يستغرق بعض الوقت، ومن جهة أخرى قد تكون النتائج خفية.

بعد تدخل روسيا في سنة 2016، حذر الديمقراطيون نظراءهم الجمهوريين مرارًا وتكرارًا من أن التدخل الانتخابي من شأنه أن يؤثر على الجهتين

في المقابل، حذر المسؤولون التنفيذيون للأمن موظفي اللجنة الوطنية الديمقراطية في رسالة إلكترونية هذا الأسبوع من إمكانية استهداف القراصنة الإيرانيين لحسابات بريدهم الإلكتروني من خلال ما يسمى

بالخداع الإلكتروني، حيث يحاول القراصنة استدراج ضحيتهم للضغط على رابط أو مُرفق ضار. ويمكن أن يوفر هذا الرابط أو المُرفق فرصة للمهاجمين للولوج إلى شبكة الحاسوب الخاصة بالضحية.

يُعتقد أيضا أنه بإمكان القراصنة التدخل في ميزة أمان إضافية تُعرف بالمصادقة ثنائية العامل – وهي طريقة شائعة للحفاظ على الأمان تقوم بطلب بيانات خاصة إضافة لكلمة المرور – ما يمكنهم من إنشاء حسابات مزيفة على موقع لينكد إن للزيادة في مصداقية رسائل البريد الإلكتروني الخاصة بهم.

بعد تدخل روسيا في سنة 2016، حذر الديمقراطيون نظراءهم الجمهوريين مرارًا وتكرارًا من أن التدخل الانتخابي من شأنه أن يؤثر على الجهتين، كما أن القراصنة الذين ترعاهم الدولة قد لا يسعون دائمًا إلى مساعدة المرشح الجمهوري. لكن حتى الآن، لا يزال السناتور عن ولاية كنتاكي والمتحصل على أغلبية الأصوات، ميتش ماكونيل، يرفض طرح أي مشاريع قوانين أمنية خاصة بالانتخابات. أما ترامب، فلم يعترف بعد بالتدخل الروسي في انتخابات سنة 2016 على الرغم من جمع خبراء الأمن السيبراني أدلة تثبت أن القرصنة الروسية للمنظمات المسؤولة عن حملات 2020 قيد التنفيذ.

في مقابلة سابقة، قال المسؤول الحكومي السابق وخبير الأمن السيبراني بمركز الدراسات الاستراتيجية والدولية في واشنطن جيمس أ. لويس، إن التدخلات الإلكترونية، حتى من قبل روسيا، لن تفيد بالضرورة الرئيس ترامب في انتخابات 2020. وأضاف لويس أن الروس وصلوا لاستنتاج مفاده أنه طالما أن ترامب لا يزال في منصبه، فإن العلاقات الأمريكية الروسية ستبقى جامدة. في خصوص هذا الموضوع، أفاد خبراء الأمن السيبراني المتخصصون في المعلومات المضللة بأنهم شهدوا العديد من حملات التضليل المنسقة التي تهدف إلى التأثير في حملة 2020.

قالت بعض شركات الأمن السيبراني إنها تشهد ما يمكن أن يكون المراحل الأولى من مجموعة من الهجمات الإلكترونية على الحملات السياسية الأمريكية من قبل الدول القومية

قالت سيندي أوتيس، مديرة وحدة التحليل في "نايسوس"، وهي شركة للأمن السيبراني في الإسكندرية (فرجينيا) إن "الجزء الأكبر من هذا التضليل نشأ محلياً، حيث كانت الدول القومية الأخرى تراقب هذه العمليات المحلية عن كثب، لكن يبدو أنها بصدد التراجع". وأضافت أوتيس: "لقد رأينا الكثير من الروايات المضللة على الصعيد الداخلي، لكن من المحتمل أن تحاول الدول القومية تضخيمها كما فعلت روسيا سنة 2016. لكن مع بقاء الكثير من المرشحين في الانتخابات، يبدو أن هذه الدول ستنتظر قبل أن تضع كل جهودها في اتجاه واحد".

في السياق ذاته، قالت بعض شركات الأمن السيبراني إنها تشهد ما يمكن أن يكون المراحل الأولى من مجموعة من الهجمات الإلكترونية على الحملات السياسية الأمريكية من قبل الدول القومية. ففي تموز/ي وليو، أطلع نائب رئيس شركة مايكروسوفت، توم بيرت، جمهورا في مؤتمر منتدى أسبن الأمني أن مايكروسوفت تملك دليلا على أن روسيا وإيران وكوريا الشمالية تعتبر الأكثر نشاطا في مجال الهجمات إلكترونية.

يعقد كبير موظفي الأمن باللجنة الوطنية الديمقراطية، بوب لورد، من حين لآخر مؤتمرات فيديو مع أعضاء الحملة الرئاسية لإبقائه على اطلاع على آخر المخاطر

وتجدر الإشارة إلى أن عددا قليلا من الحملات الانتخابية الرئاسية الديمقراطية استأجرت موظفا للأمن السيبراني بدوام كامل بسبب قلة التمويل. وقد اعتمدوا في المقابل على نصيحة اللجنة الوطنية الديمقراطية وشركة التكنولوجيا الديموقراطية "ديجي دامز"، التي تأسست إثر الحملة الرئاسية لسنة 2016.

يعقد كبير موظفي الأمن باللجنة الوطنية الديمقراطية، بوب لورد، من حين لآخر مؤتمرات فيديو مع

أعضاء الحملة الرئاسية لإبقائه على اطلاع على آخر المخاطر. وقد أوصت اللجنة أيضًا بأن يكون لكل حملة نقطة اتصال للأمن السيبراني وأن يتم إرسال رسائل دورية وفي حالات الطوارئ. بغض النظر عن ملايين الدولارات التي جمعتها، تواجه كل حملة قرارًا صعبًا عند تشكيل فريق الأمن السيبراني: تعتبر هذه التكنولوجيا والخبرات غالية الثمن، والأمر سيان بالنسبة للعمل الميداني.

كما أوضح كبير المستشارين السابق في حملة بيرني ساندرز لسنة 2016، تاد ديفاين، أن "الحملات تستمر فقط حتى يوم الانتخابات أو عندما يخرج مرشحك. فإذا كنت تنفق الكثير على الأمن السيبراني في حين تنفق أقل على الاتصال بالناخبين فستنتهي بعدم إجراء اتصالات كافية بهم. هذا هي المعضلة التي تدور حولها الحملات الانتخابية". وأضاف ديفاين: "السياسة عمل محفوف بالمخاطر وعليك أن تقرر ما هي المخاطر التي سوف تتحملها".

المصدر: نيويورك تايمز