امريكا والصين.. هل يخوضان حربا إلكترونية باردة؟؟

2015-06-10شبكة النبأ

مثلما يتطور كل شيء في الحياة، فقد تطورت الحروب وتضاعفت وسائلها، وتنوعت وتعددت أشكالها، فلم تعد المبارزة وجها لوجه سمة او تقليدا للحرب الحديثة، ولم تعد هناك قواعد شرف يحتكم إليها المتحاربون كما كان الامر في حروب العصور الغابرة، كذلك لم تعد الحرب تتعلق بالقضاء على العنصر البشري، بقدر ما يتعلق الامر باستخدام الطرق والوسائل الالكترونية التي باتت تتحكم بتحريك جحافل من الآلات بمختلف المهام والاحجام، فمنها صغيرة، واخرى متوسطة وكبيرة، تمشي على الارض او تمخر عباب البحر او تجوب الفضاء كالطائرات بأنواعها، ومنها المسيّرة، والتي تقاد بطيارين مهرة، فباتت انظمة التحكم الالكترونية هي التي تقود الحروب، كما ان هناك حربا من نوع جديد، تعتمد اسلوب اختراق شبكات الانترنيت للحكومات القوية ومؤسساتها المحكمة، كما هو الحال مع البنتاغون الامريكي، الذي بات يتعرض على نحو دائم الى هجمات فايروسية متكررة، يقوم بها متسللون من دول عدة، فقد اتهمت مؤخرا امريكا الصين اكثر من مرة، بهذا النوع من الجومات الالكترونية، كذلك قام متسللون روس باختراق شبكات الانترنيت الامريكية، حتى وصل الامر بالحكومة الامريكية ومؤسساتها أن تتخذ اجراءات سريحة وصارمة، من باب التحصين ومواجهة هذه الهجمات بأنواعها، فضلا على التفكير بشن هجمات مقابلة على شبكلت الانترنيت للدول الاخرى كمحاولة او نوع من الحلول لمواجهة حالات الاختراق التي تتعرض لها، لذلك باتت هناك تصريحات يطلقها مسؤولون على مستوى رفيع من حكومات بلدان قوية كالصين وامريكا، يشكون فيها من هذا النوع من الهجمات، ويطلقون اتهامات متبادّلة ضد بعضهم، حتى وصل الامر بأحد المسؤولين الامريكان الى وصف الهجومات الالكترونية على شبكة الانترنيت الامريكية، (بحرب باردة من نوع آخر) تهدف الى خرق حسابات سرية لشخصيات مهمة وقادة كبار.

المتسللون وكنز اختراق شبكات الكمبيوتر

وفي هذا السياق، يعد الهجوم الالكتروني الكاسح الذي تعرضت له شبكات الكمبيوتر الاتحادية الامريكية الاسبوع الماضي الأحدث ضمن طوفان من الهجمات التي يشتبه بأن متسللين صينيين

قاموا بها بغية انتزاع بيانات شخصية وأسرار صناعية وخطط أسلحة من حاسبات الحكومة والقطاع الخاص. وكشفت ادارة الرئيس باراك اوباما يوم الخميس الماضي عن اختراق أنظمة الكمبيوتر الخاصة بمكتب شؤون العاملين وقالت إن السجلات الخاصة بأكثر من أربعة ملايين موظف اتحادي حالي وسابق ربما تكون قد تعرضت للاختراق.

وقال مسؤولون أمريكيون تحدثوا شريطة عدم نشر اسمائهم إنهم يعتقدون ان المتسللين مقرهم الصين لكن واشنطن لم تتهم بكين علانية في وقت يحتدم فيه التوتر بينهما بشأن مزاعم صينية بالسيادة على مناطق ببحر الصين الجنوبي. ونفت الصين تورطها في الهجمات بحسب رويترز.

وهذه ثاني عملية اختراق خلال أقل من عام تتعرض لها شبكات الكمبيوتر الامريكية الخاصة بمكتب شؤون العاملين وهو مكتب الأفراد بالحكومة الاتحادية. وارتبط الاختراق الاول بسرقات سابقة لبيانات شخصية من ملايين السجلات في شركة انثيم ثاني أكبر شركة امريكية في مجال التأمين الصحي -وهو الهجوم الذي ألقيت بالمسؤولية عنه على متسللين من الصين- وشركة بريميرا بلو كروس التي تقدم خدمات الرعاية الصحية.

وقال روب ايجريشت وهو المؤسس المشارك والرئيس التنفيذي لشركة انتليسيكيور الخاصة للامن الالكتروني ومقرها دنفر "إنها صورة مختلفة من الحرب الباردة في هذه المرحلة". وقال إن شركته شهدت تصاعدا في الهجمات على شبكات القطاع الخاص من جانب صينيين خلال الاشهر الثلاثة الأخيرة. وكان الهجوم الاحدث لم يكشف النقاب عنه من قبل وتعرضت له مجموعة أمريكية تعمل في مجال المستحضرات الدوائية ما كبد الشركة خسائر تقدر بمئات الملايين من الدولارات تتعلق بابحاث حساسة وجهود للتطوير.

وقال الاميرال جيمس وينفيلد نائب رئيس لجنة الاركان الامريكية المشتركة خلال مؤتمر للامن الالكتروني بالاكاديمية العسكرية في منطقة وست بوينت الشهر الماضي إن خصوما لواشنطن مثل الصين وروسيا يصعدون من هجماتهم بوتيرة سريعة على الشبكات العسكرية الامريكية. وعرضت الصين في السنوات الاخيرة طائرتين مقاتلتين حديثتين من نوع ستيلث يقول محللون إنها تشبه في امكاناتها المقاتلتين إف-22 وإف-35 اللتين تنتجهما شركة لوكهيد مارتن التي ضاعفت من جهودها

الامنية بعد هجوم "كبير ومتقن" على شبكات الكمبيوتر الخاصة بها عام 2011 . واضاف اعضاء بالكونجرس الامريكي تمويلا حجمه 200 مليون دولار الى مشروع موازنة عام 2016 المالية لتمويل دراسة تتناول نقاط الضعف في مجال الامن الالكتروني لانظمة الاسلحة الامريكية.

ويقول مسؤولون حكوميون امريكيون ومحللون في حقل الامن الالكتروني إن المتسللين الصينيين يستخدمون اساليب تقنية متطورة لإنشاء قاعدة بيانات ضخمة يمكن استخدامها في اغراض التجسس التقليدية مثل تجنيد الجواسيس أو تسهيل التسلل الى البيانات المؤمنة على الشبكات الأخرى. ومنح الهجوم الأخير المتسللين القدرة على الوصول الى كنز دفين من البيانات الشخصية منها تواريخ الميلاد وارقام بطاقات التأمين الاجتماعي والعناوين السابقة والتراخيص الامنية. وتساعد جميع هذه المعلومات المتسللين على تحقيق اغراض معينة منها الحصول على كلمات السر الخاصة بالمواقع الالكترونية التي قد تفتح الباب على مصراعيه وصولا الى بيانات عن انظمة التسليح وبيانات البحوث الاخرى.

تعزيز الآمن الالكتروني في امريكا

من جهته حض البيت الابيض الكونغرس على تمرير قوانين جديدة لامن الانترنت مشيرا الى خرق امني واسع لنطاق كشف عنه مؤخرا لدعم حججه الداعية الى الاصلاح. واستغل حلفاء الرئيس باراك اوباما خبر قرصنة المعطيات الشخصية لاربعة ملايين موظف حكومي، للضغط من اجل اقرار تشريع لا يزال عالقا في الكونغرس الذي يهيمن عليه الجمهوريون. وقال المتحدث باسم البيت الابيض جوش ارنست "الحقيقة هي اننا بحاجة الى ان يخرج الكونغرس من العصور الوسطى الى القرن الحادي والعشرين لضمان ان يكون لدينا الدفاعات الضرورية من اجل حماية نظام الكتروني حديث". كما انضمت نائبة رئيس لجنة الاستخبارات في مجلس الشيوخ الديموقراطي ديان فاينشتاين الى دعوة البيت الابيض.

وقالت فاينشتاين "يجب ان يتحرك الكونغرس" لتسريع الابلاغ باي اختراق للامن الالكتروني وتعزيز التعاون بين الحكومة والشركات الخاصة. واضافت انه "من المستحيل ان نستهين بهذا التهديد" بحسب فرانس بريس. وتابعت ان "مئات مليارات الدولارات، والبيانات الخاصة لكل اميركي، حتى

امن البنية التحتية الحيوية مثل شبكة الكهرباء ومحطات الطاقة النووية والمياه الصالحة للشرب، معرضة للخطر".

واقرت الحكومة الاميركية الخميس بانها رصدت عمليات قرصنة معلوماتية طالت المعطيات الشخصية لاربعة ملايين موظف فدرالي، وقالت صحيفة واشنطن بوست ان قراصنة صينيين يقفون وراء العملية. وتضمن التوغل الالكتروني الذي طال مكتب ادارة شؤون الموظفين، سجلات 750 الف موظف مدني من وزارة الدفاع. وذكرت صحيفة نيويورك تايمز الجمعة ان المفتش العام لوزارة الدفاع كان حذر في تشرين الثاني/نوفمبر ان قاعدة بيانات المكتب كانت عرضة لهجمات الكترونية. وافادت الصحيفة انه تزامنا مع هذا التحذير، نهب قراصنة عشرات الاف من الملفات التي تحتوي على تصاريح امنية، مما شكل اساسا للهجوم على نطاق واسع الذي كشف عنه. ونقلت الصحيفة عن مسؤول كبير قوله ان "السؤال ليس كيف تمت سرقة البيانات من من قبل الصينيين، بل لماذا استغرق الصينيين كل هذا الوقت؟". وتتهم الولايات المتحدة الصين مرارا بشن حرب الكترونية في السنوات الاخيرة، وهو ما تنفيه بكين دائما.

بيانات قديمة تعرضت للقرصنة

وفي سياق متصل قال مسؤولون أمريكيون إن بيانات سرقها من أجهزة كمبيوتر حكومية أمريكية من يشتبه أنهم متسللون صينيون شملت موافقات أمنية وتحريات ترجع الى ثلاثة عقود مضت مما يبرز حجم واحدة من أكبر الهجمات الالكترونية المعروفة على الشبكات الاتحادية. وقال مسؤول طلب عدم نشر اسمه إن هذه مسألة خطيرة وأضاف "البيانات ترجع الى عام 1985... هذا يعني أن من المحتمل أن تكون لديهم معلومات عن متقاعدين ويمكنهم أن يعرفوا ماذا فعلوا بعد أن تركوا الحكومة." وأضاف المسؤول أن الحصول على معلومات من كمبيوتر مكتب شؤون العاملين مثل تواريخ الميلاد وأرقام الضمان الاجتماعي والمعلومات البنكية يمكن أن يساعد المتسللين على تجربة كلمات السر المحتملة في مواقع أخرى يحتوي بعضها على معلومات عن أنظمة تسليح خطيرة.

فيما قال متحدث باسم وزارة الخارجية الصينية إن هذه الاتهامات تكررت في الآونة الأخيرة وإنها

غير مسؤولة. وأضاف أن هجمات المتسللين تكون عادة من الخارج ويصعب تتبع مصدرها. وقال المتحدث باسم البيت الأبيض جوش إيرنست إنه لم يتضح بعد من المسؤول عن هذا الاختراق لكنه أشار إلى أن أوباما ومساعديه يثيرون مع نظرائهم الصينيين بشكل دوري بواعث قلقهم بشأن التصرفات الصينية في مجال الانترنت.

قراصنة روس يخترقون شبكة للبيت الأبيض

من ناحية اخرى تمكن قراصنة روس في العام الماضي من الاطلاع على رسائل إلكترونية للرئيس الأمريكي باراك أوباما بعد اختراقهم شبكة معلوماتية غير سرية للبيت الأبيض، حسب ما كشفت عنه صحيفة "نيويورك تايمز"، كما اخترقوا أيضا الشبكة غير السرية لوزارة الخارجية الأمريكية.

وذكرت صحيفة "نيويورك تايمز" أن قراصنة روس تمكنوا في العام الماضي من قراءة رسائل إلكترونية أرسلها الرئيس الأمريكي باراك أوباما وأخرى تلقاها، وذلك بعد أن تمكنوا من اختراق شبكة ملعوماتية غير سرية للبيت الأبيض. وكان مسؤولون أمريكيون أقروا في مطلع نيساذ/أبريل الجاري بحصول "حادث" في مجال الأمن المعلوماتي في نهاية العام الماضي، لكنهم رفضوا تأكيد صحة معلومات ذكرت أن قراصنة روس يقفون خلف هذه الهجمات الإلكترونية. وقالت الصحيفة، نقلا عن مسؤولين أمريكيين على علم بالتحقيقات الجارية في هذه القضية، إن الهجوم الإلكتروني "كان أكثر تطفلا وأكثر مدعاة للقلق" مما تم الإقرار به رسميا. ونقلت الصحيفة عن المسؤولين اعتقادهم أن القراصنة على علاقة بالسلطات الروسية.

وبحسب "نيويورك تايمز" فإن القراصنة، الذين اخترقوا أيضا الشبكة المعلوماتية غير السرية لوزارة الخارجية الأمريكية، ونجحوا في الدخول إلى أرشيف الرسائل الإلكترونية لموظفين في البيت الأبيض يتواصل الرئيس أوباما معهم بصورة مستمرة. وفي هذا الأرشيف تمكن القراصنة من قراءة رسائل تلقاها أوباما وأخرى أرسلها، بحسب الصحيفة. الصحيفة وأضافت أن عدد الرسائل التي قرأها القراصنة غير معروف، مشيرة إلى أن حسابه البريدي لم يخترق على الأرجح بحسب فرانس بريس.

من جهة اخرى قالت شركة أمن مشاركة في التحقيقات إن حملة التجسس الالكتروني الروسية التي

تحدثت عنها وسائل الإعلام ضد أهداف دبلوماسية في الولايات المتحدة ودول أخرى استغلت ثغرتين لم تكونا معروفتين من قبل في برامج الكمبيوتر لاختراق الأجهزة المستهدفة. وقالت شركة فاير آي وهي شركة أمن أمريكية مرموقة إن عمليات التجسس استغلت ثغرة في برنامج فلاش الذي توفره شركة ادوب سيستيمز للاطلاع على المحتوى النشط وأخرى في النظام المشغل لبرامج ويندوز الخاصة بشركة مايكروسوفت. وربطت شركات أخرى بين هذه الحملة والاختراقات الخطيرة التي تعرضت لها شبكة الكمبيوتر الخاصة بوزارة الخارجية الامريكية بل تعتقد ان نفس هؤلاء المتسللين هم المسؤولون عن اختراق أجهزة كمبيوتر خاصة بالبيت الأبيض تحوي معلومات غير سرية لكنها حساسة مثل جدول تنقلات الرئيس الامريكي.

وتساعد شركة فاير آي الوكالات الاتحادية في التحقيق في هذه الهجمات لكنها قالت إنه ليس بوسعها التعليق عما اذا كان هؤلاء الجواسيس هم نفس من اخترقوا البيت الابيض لان هذا يدخل ضمن الاسرار غير المصرح بنشرها. وفي اكتوبر تشرين الاول قالت فاير آي ان مجموعة التجسس التي اطلقت عليها اسم ايهـبيـتي 28 تعمل منذ عام 2007 وانها استهدفت الملحقين العسكريين الامريكيين والمتعاقدين العسكريين ومكاتب حلف شمال الاطلسي ومسؤولين حكوميين في جورجيا ودول أخرى تهم الكرملين. وقبل ذلك التقرير بأيام تحدثت شركة ترينـد مايكرو الأمنية عن حملة أطلقت عليها اسم "عاصفة البيدق" استهدفت شبكة الكمبيوتر الخاصة بوزارة الخارجية الامريكية والمنشقين الروس وحلف شمال الاطلسي ودول شرق أوروبا بحسب رويترز.

هل تخترق ايران شبكات الكمبيوتر الاميركية

في سياق آخر اظهرت دراسة جديدة ان ايران تشكل خطرا متزايدا على شبكات الكمبيوتر الاميركية وقد نفذت هجمات وعمليات تجسس رقمية متزايدة متطورة على اهداف اميركية. وقالت الدراسة التي اجرتها شركة "نورس" الخاصة والمتخصصة في امن المعلوماتية ومعهد اميركان انتربرايز ان جهود ايران المتزايدة للقرصنة تشير الى ان النظام الايراني يبحث عن بنية تحتية ضعيفة يمكن ان يستهدفها في هجماته المعلوماتية المستقبلية. وذكرت الدراسة ان "ايران بدأت تظهر كتهديد كبير للولايات المتحدة وحلفائها في مجال المعلوماتية". واوضحت ان مهارات ايران في مجال المعلوماتية تحسنت بشكل كبير في السنوات الاخيرة كما ان ايران "اخترقت بالفعل شبكات جيدة

الحماية في الولايات المتحدة والسعودية وحصلت على معلومات حساسة ودمرتها".

واتسعت عمليات القرصنة التي اشتملت على التجسس والهجمات، رغم العقوبات الاقتصادية المفروضة على ايران والمفاوضات بين طهران والدول الكبرى بشان برنامج طهران النووي. واستندت الدراسة الى بيانات من شبكة تضم ملايين المواقع التي اقامتها شركة نورس لتبدو بمثابة مواقع حقيقية مثل تلك التي في البنوك او محطات الطاقة، والتي يمكن ان تجذب اهتمام قراصنة الانترنت بحسب فرانس بريس. واظهرت البيانات ان ايران تشن هجمات معلوماتية من داخل وخارج البلاد.

وقالت الدراسة ان شركات ايرانية حكومية من بينها شركات ترتبط بالحرس الثوري الايراني، تستضيف خوادم وغيرها من انظمة الكمبيوتر في الغرب للقيام بالهجمات الرقمية. وتابعت "ببساطة من خلال التسجيل ودفع رسم معين، فان اجهزة الامن الايرانية والمواطنين الايرانيين العاديين يستطيعون الدخول الى انظمة وبرامج كمبيوتر معقدة ومتطورة يحاول الغرب منعهم من الحصول عليها". وتعكس الدراسة تحذيرات مسؤولي استخبارات اميركيين من ان ايران حققت تقدما كبيرا في قدراتها في مجال المعلوماتية رغم ان الصين وروسيا تعتبران الاكثر مهارة في الحرب الرقمية.

البنتاغون لايتمكن من شن هجمات معلوماتية

من جهة اخرى اقر مسؤول في وزارة الدفاع الاميركية ان البنتاغون لا يمتلك حتى الان البرنامج التقني للقيام بهجمات رقمية حقيقية. واوضح اريك روزنباك كبير مستشاري وزير الدفاع الاميركي في مجال الامن الرقمي ان القيادة المعلوماتية في البنتاغون تملك "قدرات متينة بشكل كاف" في حال وقوع هجمات الكترونية. لكن هذه القيادة لا تملك في المقابل حتى الان "قدرات متينة" لقيادة حملة عسكرية لضربات الكترونية كما اضاف. واكد ان وزير الدفاع الجديد اشتون كارتر يهتم كثيرا بالمجال الرقمي وعندما تثبت الحلول المطروحة فعاليتها "سيكون الاول" في اجراء الاستثمارات الضرورية.

ومن المفترض ان تمتلك القيادة المعلوماتية في البنتاغون قوة قوامها ستة الاف عسكري متخصص

يوزعون على 133 وحدة قتالية في القوات البرية والبحرية والقوات الجوية والمارينز. وقدر البنتاغون مؤخرا انه بات في منتصف الطريق لبلوغ هذا الهدف الذي كان يفترض اصلا تحقيقه في 2016. واشار روزنباك من جهته الى تاريخ 2018. والقوة المعلوماتية للبنتاغون يفترض ان تكون قادرة على الدفاع عن الشبكات المعلوماتية العسكرية وايضا شبكات البنى التحتية المدنية الاميركية الكبرى مثل الطاقة والمياه والمالية وغيرها. كما يفترض ان تكون ايضا قادرة على القيام بتحركات هجومية ضد اعداء الولايات المتحدة بما في ذلك اهداف "غير عسكرية" مثل شبكة الكهرباء بحسب روزنباك.

لكن هذه الهجمات على اهداف مدنية ستجرى كما اوضح "بطريقة دقيقة وواضحة جدا ضمن احترام قوانين الحرب" ومع الحرص على "تجنب الاضرار الجانبية". واضاف ان وزارة الدفاع "بصدد وضع اللمسات الاخيرة على استراتيجية جديدة ستنظم انشطتها في المجال المعلوماتي من اجل الدفاع عن المصالح الاميركية ودعمها".

شبكات الجيش الإسرائيلي تتعرض للاختراق

في سياق آخر قال باحثون في مؤسسة أمنية خاصة إن متسللين تمكنوا من اختراق شبكات كمبيوتر مرتبطة بالجيش الإسرائيلي في حملة تجسس جمعت بمهارة بين برامج اختراق موجودة بالفعل وحسابات بريد الكتروني خداعية. وقال الباحثون إن الحملة المستمرة منذ أربعة أشهر وينفذها على الأرجح مبرمجون ناطقون بالعربية تظهر كيف أن الشرق الأوسط ما زال معقلا لعمليات التجسس عبر الانترنت وكيف انتشرت القدرة على تنفيذ مثل هذه الهجمات.

وقال وايلون جرانج الباحث من مؤسسة بلو كوت سيستمز الأمنية الذي اكتشف الحملة إن معظم برامج الاختراق مؤلفة من أدوات متوفرة على نطاق واسع مثل فيروس تروجان الذي يتم التحكم به عن بعد ويعرف باسم بويزون أيفي (اللبلاب السام). وأضاف أن المتسللين على الأرجح يعملون بميزانية محدودة ولم يروا حاجة لإنفاق الكثير من الأموال لكتابة شفرة مخصصة للهجوم مشيرا إلى أن معظم عملهم يبدو وأنه انصب على ما يسمى الهندسة الاجتماعية أو الخداع البشري. ووفقا لمؤسسة بلو كوت فقد أرسل المتسللون رسائل بريد الكتروني إلى عدد من الحسابات العسكرية

تزعم أنها تحمل أخبارا عسكرية عاجلة أو في بعض الحالات مقطع فيديو يظهر "فتيات جيش الدفاع الإسرائيلي" بحسب رويترز. وتضمنت بعض هذه الرسائل ملفات مرفقة فتحت مجالا لخلق أبواب خلفية تتيح للمتسللين الوصول إلى تلك الحسابات في المستقبل ووحدات نمطية يمكنها تحميل وتشغيل برامج. وأحالت متحدثة باسم وزارة الدفاع الإسرائيلية الأسئلة الى الجيش. وقال مسؤولون عسكريون إنهم "لا يعلمون بعمليات تسلل الى شبكات جيش الدفاع الإسرائيلي."

هجوم الكتروني على الصين

من جهتها قالت صحيفة صينية رسمية إن هجوما الكترونيا باستخدام برمجيات خبيثة من خوادم خارجية كان السبب وراء مشاكل في شبكة الانترنت وقعت في الصين في وقت السابق هذا الاسبوع ومنعت المستخدمين من الدخول إلى عدد من مواقع الاجنبية الشهيرة. وشكا مستخدمون لمواقع التواصل الاجتماعي انه يتم اعادة توجيههم إلى موقع البرمجيات (دابليو.بي.كي.جي دوت اورج) وموقع السفر (بي.ترافلر دوت كوم) عندما يحاولون الدخول إلى مواقع للاخبار مثل (سي.ان.ان دوت كوم) وبوابة الاخبار (ياهو دوت سي.او دوت جيه.بي) وموقع الالعاب (ران سكاب دوت كوم). وكان ذلك احدث تحدي ضمن سلسلة من التحديات واجهت الشركات والافراد عبر الانترنت في ثاني اكبر اقتصاد في العالم بحسب رويترز.

ونقلت صحيفة تشاينا ديلي التي تصدر باللغة الانجليزية عن الوكالة المسؤولة عن مراقبة سلامة الانترنت في الصين القول إن اعادة التوجيه حدث لان بعض الخوادم في الصين "تلوثت" ببرمجيات خبيثة من خوادم خارجية. وقالت الصحيفة "قال خبراء إنه سيكون من الصعب تعقب مصدر الهجوم لان من الممكن تقنيا تنفيذه بالتحكم عن بعد في الخوادم."