لا هجوم لقراصنة المعلوماتية بعد!: حقيقة أم العكس هو الصحيح

2018-02-07مروة الاسدي

لا مكان آمنا على الانترنت، بعدما ازدادت هجمات القرصنة الإلكترونية التي تهدف إلى سرقة البيانات الشخصية أو هجمات الفيروسات والبرامج الخبيثة لاختراق أجهزة الكمبيوتر، فضلا عن دخول العديد من الحكومات إلى عالم التكنولوجيا، فقد شهدت الآونة الاخيرة سلسلة غير مسبوقة من الاختراقات الأمنيّة أدّت إلى إدخال الشبكة العنكبوتيّة في دائرة الخطر، وتراجع ثقة المستخدمين بقدرات الشركات على حماية بياناتهم.

لذا باتت علميات القرصنة الإلكترونية التهديد الأكبر لمعظم دول العالم من خلال عصابات المقرصنين الدولية، حيث ان الهجمات الإلكترونية تستهدف أنظمة الشركات بشكل مباشر وكذلك الأفراد، مما يعني سباق التسليح الإلكتروني تحدٍ مُلح، ورد الفعل المؤثر يتطلب موقفا جماعيا للحكومات، وسلطات تنفيذ القانون، ومن ينظمون لوائح الصناعات، وقادة الأعمال.

يرى الخبراء في مجال أمن المعلومات إن إمكانية الاتصال غير المسبوقة التي أتاحها عصر الإنترنت، أدت إلى فوائد اجتماعية واقتصادية هائلة، لكنها في الوقت نفسه فرضت العديد من التحديات الجديدة. وفي عالمنا المتصل تمامًا، لا تزال التهديدات المتعلقة بأمن الإنترنت تواصل تطوَّرها، الأمر الذي يمنحها الأسبقية دومًا على أكثر الدفاعات تقدمًا.

ويرى هؤلاء الخبراء أدت تهديدات الأمن القائمة على الشبكة إلى انتشار عمليات سرقة الهوية والاحتيال المالي على نطاق واسع. ويعاني المستهلكون والشركات من مشاكل بالغة من جراء رسائل البريد غير المرغوب فيه، والفيروسات، وبرامج التجسس.

كما أن الاختراق الأمني يمكن أن يضر بالعلامة التجارية للشركات أو سمعتها بشكل يستحيل تدارك آثارها. وفي الولايات المتحدة، تعرقل المشاكل المتعلقة بأمن الإنترنت مسيرة التحول إلى استخدام السجلات الطبية الإلكترونية داخل البلاد. وفي الاتحاد الأوروبي، تشكِّل ثقة المستهلكين فيما يتعلق

بأمن الإنترنت وحماية البيانات عائقًا أمام التوسع السريع للتجارة الإلكترونية عبر حدود الدول الأعضاء.

واستهدف قراصنة الإنترنت مؤسسات مالية كبرى حول العالم من بينها بنك جيهـبي مورجان أكبر بنك في الولايات المتحدة ومصارف أصغر حجما مثل بنك ديل اوسترو في الإكوادور وبنك تين فونج في فيتنام.

وقال محللون أمنيون إن الحكومات الأجنبية قد تستفيد من الحصول على معلومات من داخل مجلس الاحتياطي الاتحادي. فالصين وروسيا على سبيل المثال لاعبتان كبيرتان في سوق الدين الاتحادي حيث تلعب سياسة المجلس دورا كبيرا في تحديد أسعار الفائدة.

وقد شهد العالم في الآونة الأخيرة هجمات الكترونية واسعة النطاق بينها خصوصا "باد رابيت" و"نوبت بيتيا" و"وانا كراي" وهي ثلاث برمجيات تسببت بشل عمل مئات آلاف أجهزة الكمبيوتر حول العالم ودرت أموالا طائلة لقراصنة المعلوماتية.

وسيتمكن قراصنة المعلوماتية تاليا من الحاق الضرر أو التدمير الكامل لأهدافهم بدل تعطيل حركتها. أما الضحايا الجدد فقد يكونون من الشخصيات الثرية التي قد ينصبون أفخاخ لها عبر أكسسوارات متصلة بالانترنت أقل حصانة في مواجهة هذه الهجمات مقارنة مع أجهزة الكمبيوتر أو الهواتف الذكية.

فيما أماط باحثون اللثام عن مجموعة من الثغرات الأمنية التي قالوا إنها قد تتيح للمتسللين سرقة معلومات حساسة من كل جهاز حاسوب حديث تقريبا يحتوي على رقائق من إنتاج شركات إنتل كورب وأدفانسد مايكرو ديفايسيز (إيهـإمـدي) و(إيهـآر.إم هولدنجز).

في حين تسعى كبريات شركات المعلوماتية في العالم وعلى رأسها غوغل، آبل، وأمازون، إلى احتواء مشكلة ثغرتين أمنيتين في أنظمة ماك والأجهزة العاملة بنظام "آي أو إس" لمنع هجوم محتمل لقراصنة المعلوماتية، مستغلين ثغرتي "سبيكتر" و"ملتداون" تحديدا. وهما تشملان أغلب المعالجات

الصغرى المصنعة خلال السنوات العشر الأخيرة في شركات "إنتل" و"إيه ام دي" و"إيه آر ام".

الى ذلك أجمع مسؤولو الشركات المتخصصة في أمن المعلومات أنّ الحرب الإلكترونيّة ستزداد شراسة خلال هذا العام، خصوصاً الهجمات التي ستستهدف قطاعي الحكومة والمال بكافة مجالاته. كما يؤكدون أنّ المقرصنين أصبح لديهم جهات داعمة لتعزيز قدراتهم التقنيّة التي قد تؤدي إلى زعزعة ثقة القطاع التكنولوجي بكيانه، محذّرين من تراخي القطاعات التكنولوجيّة بأمن معلوماتها في المؤسسات العامة والخاصة.

2018 ستكون سنة حافلة بالهجمات الالكترونية

أكدت شركة "ماكافي" لأمن المعلوماتية في تقرير نشرته الأربعاء أن العام 2018 سيكون حافلا بالجرائم الالكترونية مع تطوير أدوات أكثر فتكا من جانب قراصنة المعلوماتية، فقد درت البرمجية الخبيثة "واناكراي" التي طاولت في أيار/مايو خدمات الصحة البريطانية ومصانع شركة "رينو" الفرنسية للسيارات وسكك الحديد في المانيا والحكومة الاسبانية، 140 مليون دولار على القراصنة المعلوماتيين. بحسب فرانس برس.

غير أن هذه الهجمات لم تكن سوى مقدمة لعمليات أكبر بحسب تقرير "ماكافي" السنوي عن المخاطر في هذا المجال لأن مجرمي المعلوماتية يطورون استراتيجيات جديدة و"نماذج اقتصادية" للحفاظ على موقع متقدم في مواجهة الأدوات الدفاعية.

وبحسب "ماكافي"، سيكون المنحى في 2018 للهجمات المنفذة "على شكل خدمات" من جانب قراصنة معلوماتية مأجورين، وأوضح المسؤول العلمي لدى "ماكافي" راج ساماني أن البرمجيات الخبيثة "يمكن أن تباع لجهات تسعى لشل عمل منافسين وطنيين أو سياسيين أو تجاريين"، وأبدت "ماكافي" قلقها أيضا من نقص الأمن في بيانات المستخدمين خصوصا المتعلقة بالأطفال والتي تجمع وتوضع في السوق من جانب مصنعي الأكسسوارات المتصلة، واعتبر معدو التقرير أن "مصنعي الأكسسوارات المنزلية المتصلة ومزودي الخدمات سيحاولون تعويض هوامشهم الضعيفة من خلال جمع بياناتنا الشخصية بدرجة أكبر، سواء بموافقتنا أم لا".

ثغرات أمنية تهدد كل الهواتف وأجهزة الكمبيوتر

قال بريان كرزانيتش الرئيس التنفيذي لإنتل في مقابلة مع شبكة (سيإنبيسي) مساء يوم الأربعاء "الهواتف وأجهزة الكمبيوتر، كل شيء سيصيبه بعض التأثير ولكن سيختلف الأمر من منتج لآخر".

وكشف باحثون من جوجل بروجيكت زيرو التابعة لمجموعة ألفابت بالتعاون مع باحثين أكاديميين وفي القطاع من عدة دول عن ثغرتين، وتؤثر الثغرة الأولى والمسماة (ميلتداون) على رقائق إنتل وتتيح للمتسللين تجاوز الحاجز بين التطبيقات التي يشغلها المستخدمون وذاكرة الكمبيوتر، مما قد يتيح للمتسللين قراءة الذاكرة وسرقة كلمات المرور السرية.

وتتعلق الثغرة الثانية التي تحمل الاسم (سبتكر) بالرقائق من إنتاج شركات (إنتل) و(إيهإم.دي) و(إيهآر.إم) ويمكن أن تسمح للمتسللين بخداع التطبيقات الخالية من الأخطاء للحصول على معلومات سرية.

وقال الباحثون إن شركتي (أبل) و(مايكروسوفت) لديهما برمجيات إصلاح جاهزة لمستخدمي أجهزة الكمبيوتر المتأثرة بالثغرة (ميلتداون). وامتنعت (مايكروسوفت) عن التعقيب ولم ترد (أبل) على طلبات للتعليق.

وفي مقابلة مع رويترز، قال دانيال جروس أحد الباحثين بجامعة جراز للتكنولوجيا والذين اكتشفوا الثغرة (ميلتداون) إنها "على الأرجح إحدى أسوأ ثغرات وحدات التشغيل المركزية المتكشفة على الإطلاق".

وقال جروس إن (ميلتداون) مشكلة أكثر خطورة على المدى القصير ولكن يمكن معالجتها تماما من خلال برامج الإصلاح، وأضاف أن الثغرة (سبتكر)، وهي الأوسع نطاقا والتي تؤثر على كافة الأجهزة الكمبيوترية تقريبا، يجد المتسللون صعوبة أكبر في استغلالها لكن يصعب إصلاحها أيضا وسوف تمثل مشكلة أكبر على المدى البعيد.

ومتحدثا إلى (سي.إن.بي.سي)، قال كرزانيتش الرئيس التنفيذي لشركة (إنتل) إن باحثي جوجل أبلغوا الشركة بالثغرات "منذ فترة" وإنها تختبر برامج إصلاح سينتجها مصنعو الأجهزة الذين يستخدمون رقائق الشركة الأسبوع المقبل. وقبل الكشف عن المشكلات، قالت جوجل عبر مدونتها إن إنتل وشركات أخرى تعتزم الإعلان عنها يوم التاسع من يناير كانون الثاني الجاري، وتم الابلاغ عن الثغرات لأول مرة بواسطة نشرة (ذا ريجستر) المعنية بالتكنولوجيا. وذكرت النشرة أيضا أن تحديثات إصلاح الثغرات قد تسبب بطء تشغيل رقائق إنتل بنسبة 5 إلى 30 بالمئة، ونفت (إنتل) أن برامج الإصلاح ستسبب بطء أجهزة الكمبيوتر التي تعتمد على الرقائق التي تنتجها، وقال المتحدث باسم (إيه.آر.إم) فيل هيوز إن برامج الإصلاح تم إرسالها بالفعل إلى شركاء الشركة ومنهم العديد من شركات الهواتف الذكية، وتأثرت رقائق (إيه.إن.دي) أيضا بواحدة على الأقل من الثغرات الأمنية ولكن يمكن إصلاحها من خلال تحديث للبرميجات، وقالت الشركة إنها تعتقد أنه "لا خطر تقريبا على منتجات (إيه.إن.دي) في الوقت الراهن".

عمالقة التكنولوجيا في سباق مع الزمن

اتسعت قائمة الشركات العالمية العملاقة في مجال المعلوماتية المتضررة من جراء ثغرتين كبيرتين هما "سبيكتر" و"ملتداون" لتشمل "أمازون و غوغل وآبل. فيما تتسارع وتيرة الخطوات المتخذة للحد من الخسائر.

وكتبت "آبل" المعروف أن منتجاتها هي عادة آمنة، على مدونتها الرسمية أن "كل أنظمة ماك والأجهزة العاملة بنظام "آي أو إس" معنية بهذه المشكلة، لكن ما من هجوم علم بحدوثه حتى الساعة".

وتعاني أغلب المعالجات الصغرى المصنعة خلال السنوات العشر الأخيرة في شركات "إنتل" و"ايه ام دي "و"ايه آر إم"، من ثغرتي "سبيكتر" و"ملتداون". وما من حاسوب أو هاتف ذكي أو جهاز لوحي يعمل من دون هذه المكونات الصغرى التي تقوم مقام مركز عصبي يوجه الأوامر للبرامج المعلوماتية.

وتختلف الثغرتان عن الإنذارات الأمنية التقليدية التي تطال عادة البرمجيات الحاسوبية وليس المكونات الصلبة في الأجهزة، وتتيح "سبيكتر" و"ملتداون" نظريا النفاذ إلى "نواة" نظام التشغيل المعلوماتي، "وصولا إلى معلومات حساسة مخزنة فيه" مثل كلمات السر، بحسب رسالة توضيحية نشرها الخميس كريس موراليس كبير المحللين الأمنيين في شركة "فيكترا نتووركس" الأمريكية للأمن المعلوماتي.

وأوضح لوك واغنر المهندس المعلوماتي في شركة "موزيلا" على مدونة المجموعة أن الثغرة تسمح "بالاطلاع على معلومات خاصة استنادا إلى محتويات إلكترونية".

خلل يشمل الأجهزة المصنعة خلال ال10 سنوات الأخيرة، وتقريبا كل الأجهزة الإلكترونية والمعلوماتية المصنعة خلال السنوات الأخيرة مجهزة برقائق قد يشوبها هذا الخلل، وخاضت كبرى مجموعات القطاع، من قبيل "أمازون" و"غوغل" و"مايكروسوفت" ومؤسسة "موزيلا" سباقا مع الوقت للحد من الأضرار، مع الإعلان عن تصحيحات للبرمجيات.

وبدأ عملاق المعالجات الصغرى "إنتل"، على غرار منافسيه "ايه ام دي" و"إيه آر ام"، بتعميم تحديثات أمنية، وأكدت "إنتل" في بيان نشر الخميس أنها ستصدر بحلول نهاية الأسبوع المقبل "تحديثات لأكثر من 90 بالمئة من المعالجات الصغرى المسوقة خلال السنوات الخمس الأخيرة".

وبغية قطع الطريق أمام قراصنة المعلوماتية، أوصت "آبل" من جهتها "بعدم تحميل تطبيقات إلا من مواقع آمنة، مثل متجر "آب ستور" وأشارت المجموعة إلى أنها قامت بدورها بنشر تصحيحات للحد من التداعيات المحتملة لثغرة "ملتداون" وتنوي إصدار المزيد عما قريب، ويرى بعض الخبراء أن الحل الوحيد لتفادي الأضرار على المدى الطويل هو استبدال المعالجات الصغرى. وشددوا أيضا على أن قرصنة هذا النوع من المعالجات تتطلب مهارات تقنية عالية جدا، ما يحد من خطر حدوثها.

مايكروسوفت تقول إن تحديثات أمنية حديثة تبطئ الأجهزة والخوادم

قالت شركة مايكروسوفت يوم الثلاثاء إن الرقع التصحيحية التي أصدرتها للحماية من الثغرتين

الأمنيتين ميلتداون وسبكتر أبطأت بعض الأجهزة الشخصية والخوادم مشيرة إلى أن نظم التشغيل المعتمدة على معالجات قديمة لشركة إنتل عانت من بطء ملحوظ في الأداء.

وقالت الشركة في تدوينة في معرض تعليقها على شكاوى من المستخدمين إن التحديثات الأمنية أبطأت بشدة بعض الأجهزة التي تعمل برقائق من إنتاج شركة إيه.إم.دي (إدفانسيز ميكرو ديفايسيز)، وتراجعت أسهم شركة انتل التي أكدت يوم الثلاثاء أنها لم تلحظ أي مؤشرات عن بطء كبير في الأجهزة 1.4 في المئة بينما تراجعت أسهم إيه.إم.دي نحو أربعة في المئة، وكان سعر سهم (إيه.إم.دي) زاد بنحو 20 في المئة في الأسبوع الماضي نتيجة تكهنات من المستثمرين بأن الشركة المصنعة للرقائق الالكترونية قد تنتزع حصة سوقية من انتل التي تعرضت منتجاتها لمعظم الثغرات الأمنية.

وقال تيري ميرسون المسؤول التنفيذي في مايكروسوفت في تدوينة "نحن (وغيرنا في القطاع) علمنا بهذه الثغرة منذ عدة أشهر بناء على اتفاق بعدم إفشاء أسرار وبدأنا على الفور في تطوير أدوات تصدي هندسية وتحديث البنية التحتية بخدماتنا السحابية"، وكشف باحثون أمنيون عن الثغرات في الثالث من يناير كانون الثاني بعدما أثرت تقريبا على كل جهاز كمبيوتر يحتوي على رقائق من إنتاج إنتل وإيه.إم.دي وآرم هولدنجز البريطانية، وميلتداون وسبكتر ثغرتان تفسدان الذاكرة وتمنحان المتسللين فرصة لتجاوز نظم التشغيل وبرامج أمنية أخرى لسرقة كلمات مرور ومفاتيح تشفير من معظم أنواع الأجهزة والهواتف وخوادم الخدمات السحابية.

جوجل: تحديثاتنا الأمنية لم تتسبب في بطء الأنظمة

قالت شركة جوجل التابعة لمجموعة ألفابت يوم الخميس إنها طرحت في العام الماضي بالفعل تحديثات برمجية لعلاج ثغرتي سبتكر وميلتداون اللتين تصيبان الرقائق الالكترونية دون أن تتسبب في إبطاء خدماتها السحابية.

وتتيح العيوب التي تؤثر على رقائق إلكترونية من إنتاج انتل و(إيه.إم.دي) و(إيه.آر.إم) للمتسللين الالكترونيين قراءة ذاكرة الكمبيوتر وسرقة كلمات مرور مما يضع أجهزة الهواتف والكمبيوتر

والخوادم جميعها فعليا في خطر.

وقالت جوجل إنها بدأت في طرح تحديثات لمواجهة ميلتداون وسبكتر في سبتمبر أيلول وطورت بحلول ديسمبر كانون الأول تحديثا لنوع آخر من سبكتر، يعد إصلاحه أشد صعوبة، دون إبطاء أنظمة التشغيل.

وذكر بن ترينور سلوس المسؤول التنفيذي في جوجل في تدوينة "ربما كانت هذه المجموعة من الثغرات الأصعب في إصلاحها خلال عشر سنوات".

كانت شركة مايكروسوفت قالت إن تحديثات تصحيحية أصدرتها للحماية من الثغرات الأمنية أبطأت بعض الأجهزة الشخصية والخوادم مشيرة إلى أن نظم التشغيل المعتمدة على معالجات قديمة لشركة إنتل عانت من بطء ملحوظ في الأداء.

وقالت الشركة في تدوينة في معرض تعليقها على شكاوى من المستخدمين إن التحديثات الأمنية أبطأت بشدة بعض الأجهزة التي تعمل برقائق من إنتاج شركة (إيه.إم.دي).

تسلل جماعة أنونيموس للبريد الإلكتروني

تجري الشرطة الإيطالية تحقيقا في تسلل جماعة أنونيموس إلى حسابات البريد الإلكتروني لموظفين حكوميين ونشرها لوثائق حصلت عليها من تلك الحسابات، ونشرت أنونيموس المتخصصة في التسلل الإلكتروني على مدونتها الإيطالية لقطة شاشة لرسالة بريد إلكتروني، يزعم أنها أرسلت من عنوان بريد إلكتروني حكومي إلى موظف في مكتب رئيس الوزراء، تحتوي على أسماء فريق حراسة أمني مرافق لرئيس الوزراء الإيطالي باولو جنتيلوني أثناء تفقده لموقع سيزورة هذا الأسبوع.

وقالت الشرطة في بيان يوم الثلاثاء إن الشرطة المتخصصة كشفت هذا التسلل يوم السبت، وهو اليوم الذي نشرت فيه أنونيموس تدوينتها، وبدأت التحقيق على الفور، وذكر البيان أن عناوين

البريد الإلكتروني والوثائق جرى الحصول عليها من صندوقي البريد الشخصي لموظف في وزارة الدفاع ورجل شرطة.

كما نشرت جماعة أنونيموس رسالة تحتوي على الترددات اللاسلكية التي سيجري استخدامها أثناء زيارة جنتيلوني إلى بروكسل والأوامر التي صدرت إلى شرطة العاصمة الإيطالية بشأن التعامل مع المظاهرات.

ونشرت أيضا قسائم دفع ونسخا من وثائق هوية شخصية وتفاصيل رواتب عسكريين. وقال مصدر في التحقيق إنه لا يزال مستمرا لكنه لم يتوصل حتى الآن سوى لعنواني البريد الإلكتروني اللذين جرى التسلل إليهما، وأكدت وزارة الدفاع عدم وجود "فجوة" في نظم المعلومات لديها مضيفة أن المادة المنشورة كانت شخصية وعثر عليها في صناديق البريد الخاصة بموظفين في الوزارة، وقالت "لم يتم بأي شكل من الأشكال سرقة أي معلومات رسمية...أو بيانات سرية".

متسللون الكترونيون حاولوا سرقة 55 مليون روبل من بنك روسي

-قالت صحيفة كومرسانت نقلا عن مصادر مطلعة إن متسللين الكترونيين حاولوا سرقة 55 مليون روبل (940 ألف دولار) من بنك جلوبكس الروسي المملوك للدولة باستخدام نظام سويفت لتحويلات الأموال بين البنوك.

ونقلت الصحيفة عن المصادر قولها إن البنك رصد الهجوم الالكتروني وتمكن من منعه جزئيا، ونتيجة لذلك سحب المتسللون حوالي 100 ألف دولار فقط.

وأبلغ مسؤول بالبنك الصحيفة أن الهجوم نفذ الأسبوع الماضي وأن أموال الزبائن لم تتأثر. وامتنع البنك عن الإدلاء بمزيد من التعليقات للصحيفة.

وفي وقت سابق هذا الأسبوع ذكرت كومرسانت أن متسللين الكترونيين هاجموا بنكا روسيا وسحبوا أموالا عبر نظام سويفت. ولم تذكر اسم البنك في ذلك الوقت.

وفي اليوم الذي نشرت فيه الصحيفة تقريرها الأول في 19 ديسمبر كانون الأول قال فرع سويفت في روسيا (روس سويفت) إنه لا يوجد دليل على أي دخول غير مرخص إلى شبكة سويفت أو خدمات التراسل، ووفقا للموقع الالكتروني لروس سويفت فإن حوالي 500 بنك ومنظمة في روسيا يستخدمون نظام سويفت.

أمريكا توجه اتهامات لرومانيين لمزاعم اختراقهما كاميرات شرطة واشنطن

قالت وزارة العدل الأمريكية في بيان يوم الخميس إن الولايات المتحدة وجهت اتهامات لرومانيين بزعم اختراقهما لكاميرات المراقبة الإلكترونية الخاصة بشرطة واشنطن في إطار مؤامرة متعلقة ببرمجيات الفدية الخبيثة.

وأضافت الوزارة أن المتهمين اعتقلا في رومانيا في 15 ديسمبر كانون الأول بسبب الواقعة التي قالت إنها عرضت أجهزة الكمبيوتر المرتبطة بكاميرات الشرطة للخطر في الفترة من التاسع وحتى 12 يناير كانون الثاني قبل أيام من تنصيب الرئيس دونالد ترامب.

وقال البيان "تلك القضية كانت لها أولوية قصوى بسبب تأثيرها على مهمات الحماية التي يقوم بها الحرس الرئاسي وتأثيرها المحتمل على الخطة الأمنية في التنصيب الرئاسي في 2017".

وأشار البيان إلى أن المتهمين خططا أيضا لإرسال برمجيات فدية خبيثة إلى 179 ألف بريد إلكتروني. وقال "التحقيق حدد أيضا ضحايا بعينهم تلقوا تلك البرمجيات وتعرضت خوادمهم للاختراق خلال المخطط".

وقالت الوزارة إن الاتهامات الموجهة لهما تشمل التآمر لارتكاب احتيال إلكتروني ولارتكاب أشكال متعددة من الاحتيال عبر الكمبيوتر وهي اتهامات عقوبتها القصوى السجن 20 عاما.

اتهام أمريكي بالقرصنة الإلكترونية على الآلاف لأكثر من 15 عاما

اتهم أمريكي بالتجسس على آلاف الأشخاص من خلال اختراق أجهزة الكمبيوتر الخاصة بهم لأكثر من 15 عاما، واتهمت وزارة العدل الأمريكية فيليب دوراشينسكي بتصميم برامج خبيثة للتسلل إلى أجهزة كمبيوتر الضحايا.

وأفادت تقارير بالعثور على بيانات مسروقة وصور وملفات صوتية مزعومة سجلت سرا، ويواجه دوراشينسكي اتهامات بانتهاك القوانين الأمريكية الخاصة بالاحتيال وسوء استخدام أجهزة الكمبيوتر وسرقة الهويات.

وإضافة إلى ذلك، يواجه الأمريكي تهما بإنتاج مواد إباحية للأطفال نظرا لأن عددا من ضحاياه كانوا من القاصرين، وبلغ عدد التهم الموجهة إليه 16 تهمة.

وقال ستيفن أنتوني من مكتب التحقيقات الفيدرالي (إف بي آي): "دوراشينسكي متهم باستخدام مهاراته المتطورة في أجهزة الكمبيوتر والإنترنت بسوء نية، وتعريض أنظمة كثيرة وأجهزة الأفراد للخطر".

وقال أنتوني إن كثيرا من المنظمات التي يُعتقد بأن دوراشينسكي قد اخترقها تبادلت المعلومات مع إف بي آي وغيره من وكالات إنفاذ القانون للمساعدة في كشف المسؤولين الذين يقفون وراء الهجمات الإلكترونية.

وإلى جانب الأفراد، ذكرت تقارير أن دوراشينسكي اخترق أجهزة مدارس وشركات وأحد أقسام الشرطة وإحدى شركات وزارة الطاقة الأمريكية، ويُطلق على البرنامج الخبيث المستخدم في اختراق الأجهزة، على رأسها أجهزة أبل ماك المكتبية واللوحية، "فروت فلاي"، واكتشف البرنامج في بداية عام 2017، وتسبب في إرباك الباحثين وذلك سبب غموض الطرق التي مكنت البرنامج من اختراق الأجهزة.

المصارف الهولندية ودائرة الإيرادات الحكومية تتعرض للقرصنة

أكدت أكبر ثلاثة مصارف في هولندا الاثنين تعرضها إلى هجمات إلكترونية خلال الأسبوع الماضي، ما أدى إلى حجب مواقعها وخدماتها المصرفية عبر الإنترنت. ولم تسلم دائرة الإيرادات الهولندية من محاولة القرصنة، إذ تعرضت إلى هجوم مشابه ولكنه استمر لفترة وجيزة قبيل أن تستعيد خدماتها سريعا.

أعلنت أكبر ثلاثة مصارف في هولندا الاثنين تعرضها إلى عدة هجمات إلكترونية الأسبوع الماضي ما منع الوصول إلى مواقعها وخدماتها المصرفية عبر الإنترنت، وتعرضت دائرة الإيرادات الهولندية إلى هجوم مشابه استمر فترة وجيزة قبل أن تستعيد خدماتها سريعا، وفقا لمتحدث باسمها.

وتعرضت بعض المصارف الأخرى إلى هجوم من شأنه أن يؤدي إلى حجب الخدمة على الشبكة العنكبوتية، منها أبرز مصرف هولندي (آي إن جي)، فيما تعرض ثالث أكبر مقرض "إيه بي إن إمرو" إلى ثلاثة هجمات خلال عطلة نهاية الأسبوع وسبعة خلال الأسبوع الماضي، وفقا لما أفادت به وسائل إعلام هولندية.