

الاختراق الإلكتروني: حرب القرن الواحد والعشرين

2017-12-24 مروة الاسدي

في الآونة الأخيرة بزغ عصر حروب الإنترنت وبشكل كبير وخطير فقد تبين من الدوافع التي أدت إلى شن الهجمات الإلكترونية أنها نابعة من أغراض سياسية، حيث بدأت العديد الدول تعد العدة للتصدي لمثل هذه الهجمات ولشن أخرى مضادة عبر الإنترنت، فقد حذر الخبراء من ان الفترة المقبلة ستشهد حرب جديدة هي حرب التقنيات الإلكترونية التي أصبحت اليوم واقع ملموس يثير قلق الكثير من دول العالم و العديد من المسؤولين وغيرهم من أصحاب الشركات ورؤوس الأموال ممن يخشون الوقوع بأيدي قرصنة الانترنت سواء كانوا أفرادا ام مؤسسات استخباراتية حكومية، تسعى الى الحصول على بعض المعلومات المهمة عن الأعداء وتهدف الى تدمير تقنياتهم من خلال الهجمات الفايروسية المدمرة، في الآونة الأخيرة اجتاحت العالم أكبر موجة قرصنة عرفتھا الدول حديثاً، بعدما وجدت أكثر من 150 دولة حول العالم نفسها تحت رحمة سيل من الهجمات الإلكترونية غير المسبوقة، والتي أثرت على أداء العديد من المؤسسات والمنظمات، حتى إن بعض المستشفيات والمدارس والجامعات لم تسلم من هجوم برنامج الفدية الخبيثة.

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

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.

وفقا للخبراء في الامن الإلكتروني يتضح من السابق أن العالم مقبل على حرب إلكترونية يشترك فيها الأفراد ليس فقط حصراً على الدول والحكومات فهذه الحروب أعلنت من شأن الأفراد في

اسءءءام أءوءاء وءءنولوجفا الاءءال الءءفة على كافة الأصءءة وءبفن للءول والءكوماء أن شرأ مسءطفراً فآءف ءءاههم عن طرفق ءلك الأءوءاء ءءف قاموا بءءوفرها وءءهءوها بالرعافة؁ إلى أن ءءلوا فف مرءلة مواءهة لن ءءءهف بأف ءال على المءى القرفب.

وعلفه أصبح الءوف من ءرب الإنءرنء كبفراف فف الءفمقراطفااء الغربفة بعء أن اكءشف ءهاز الاسءءباراء الأمرفكف أن قرالصنة إنءرنء روس عملوا بطرفقة مسءهءفة لفرؤءروا على ءملة الانءءباب الرءاسفة الأمرفكفة لصالء ءونالء ءرامب. هءه المزاءم وصفها ءرامب بـ"السءففة" فف مقابلة أءرفها معه قناة فوكس نفوز. ومع ءلك فءفر الءعم الانءءبابف المءءمل من قبل روسفا القلق لفس لءى الرأف العام الأمرفكف فقط. إء فرى البعم أن المسءشارة الألمانية أنءفلا مفركل سءكون الضءفة القاءمة لقرالصنة الانءرنء الروس. فما مءى واقعة هءا الءطر؟ وهل سفرصء فف المسءءبل هءا السءكل من أشكال الءرب الهءفنة سلاءا رءفسفا فف الصراع من أجل كسب الرأف العام؟

ففسبوك ومافرورسوفء أءبءءا هءماء إلكءرونفة كورفة شمالفة

قال مسؤول فف البفء الأبيض إن شركءف ففسبوك ومافرورسوفء أءبءءا عءءا من ءهءفءاء الإلكءرونفة الكورفة الشمالفة الأسبوع الماضف وءلك فف الوقت الءف أنء فف الولافاء المءءة علانفة باللائمة على بفونءفانء فف هءوم إلكءرونف وقع فف مافو أفار وأصاب شبكاء الكمبفوتر فف مسءشففااء وبنوك وشركاء أءرى بالشلل.

وقال ءوم بوسرف مسءشار البفء الأبيض للأمن الءاءلف إن "ففسبوك ءءفء ءساباء مما أءى إلى وقف ءءنففء العملف لهءماء إلكءرونفة مسءمرة كما اءءء مافرورسوفء إءراءاء لإءباط هءماء قائمة لفس فقط هءوم وانا كراف فف باءئ الأمر".

ولم فءم بوسرف ءفاصل بشأن إءراءاء الشركءفن الأمرفكءفن العملاقءفن لءنه قال إن الءكومة الأمرفكفة ءعء الشركاء الأءرى إلى ءءعاون فف مءال الءفاع عن الأمن الإلكءرونف؁ وءاءء ءصرفءاء بوسرف ءلال مؤءمر صءفف بالبفء الأبيض أنءف ءلاله باللوم على كورفا الشمالفة فف هءوم وانا كراف الءف أصاب مءاء الآلاف من أءهزة الكمبفوتر فف أكثر من 150 ءولة قائلاف إن

الحكومة الأمريكية لديها دليلا واضحا على مسؤولية كوريا الشمالية. ولم يوضح هذا الدليل، وجاء الاتهام الأمريكي في وقت زادت فيه حدة التوتر مع كوريا الشمالية بسبب برامج أسلحتها النووية والصاروخية. بحسب رويترز.

وأكد متحدث باسم فيسبوك أن الشركة حذفت الأسبوع الماضي حسابات لها صلة بمجموعة للقرصنة الإلكترونية مرتبطة بكوريا الشمالية تسمى (لازاروس جروب) "لجعل ممارسة أنشطتهم أكثر صعوبة"، وقال المتحدث إن الحسابات كانت شخصية في معظمها ومزيفة وكانت تستخدم لإقامة علاقات مع الأهداف المحتملة.

وقالت فيسبوك إنها أخطرت أيضا الأشخاص الذين كانوا على اتصال بهذه الحسابات، وقال براد سميث رئيس مايكروسوفت في تدوينة إن الشركة عطلت الأسبوع الماضي برنامجا ضارا كانت (لازاروس جروب) تعتمد عليه وقامت بتنظيف أجهزة كمبيوتر عملاء أصابها هذا البرنامج و"عطلت حسابات كانت تستخدم لمواصلة الهجمات الإلكترونية"، وقال سميث إن هذه الخطوات اتُخذت بعد التشاور مع عدة حكومات لم يكشف النقاب عنها ولكنه قال إن قرار مايكروسوفت كان مستقلا.

مخابرات ألمانيا تكشف النقاب عن حسابات تواصل اجتماعي تعمل واجهة للمخابرات الصينية

نشر جهاز مخابرات ألماني تفاصيل حسابات تواصل اجتماعي يقول إنها واجهات فتحتها المخابرات الصينية لجمع معلومات شخصية عن مسؤولين وساسة ألمان، واتخذ جهاز المخابرات الداخلية الألماني خطوة غير معتادة بإعلان أسماء صفحات أفراد يقول إنها وهمية ومنظمات وهمية، وذلك لتحذير الشخصيات العامة من مخاطر تسريب معلومات شخصية مهمة عبر مواقع التواصل الاجتماعي.

وقالت المخابرات "أجهزة المخابرات الصينية تنشط على مواقع إلكترونية مثل (لينكد إن) وتحاول منذ فترة استقاء معلومات وإيجاد مصادر مخابرات بهذه الطريقة" بما في ذلك السعي وراء

معلومات عن عادات وهوايات واهتمامات الساسة.

وقال الجهاز إن تسعة أشهر من البحث أظهرت أن أكثر من عشرة آلاف مواطن ألماني تلقوا اتصالات عبر موقع لينكد إن للتواصل المهني من صفحات وهمية تتخفى في شكل صفحات بحث عن خبرات ومستشارين وباحثين وأكاديميين، وأضاف "قد تكون هناك أعداد كبيرة من الأفراد المستهدفين والصفحات الوهمية التي لم تحدد بعد"، وقال لو كانغ المتحدث باسم وزارة الخارجية الصينية في بكين يوم الاثنين إن هذه الاتهامات لا أساس لها من الصحة، وأضاف "نأمل أن نتحدث وتتصرف المؤسسات الألمانية المعنية، لا سيما الإدارات الحكومية، بطريقة تنم عن المسؤولية بشكل أكبر وألا تفعل ما لا يفيد تطور العلاقات الثنائية".

وتشمل الحسابات الوهمية التي نُشرت تفاصيلها حسابا باسم "ريتشل لي" التي تعرف نفسها بأنها مسؤولة توظيف في موقع "رايز إتش آر" و"أليكس لي" وهو مدير مشروعات في مركز لدراسات التنمية الصينية الأوروبية. بحسب رويترز.

والكثير من صور الحسابات لشبان وشابات يتسمون بالأناقة والجاذبية. وقال أحد المسؤولين إن صورة حساب "ليتشيا تشين" المديرية في المركز الصيني للسياسة والاقتصاد الدوليين مأخوذة من كتيب مصور للموضة منشور على الإنترنت، وأظهرت مراجعة رويترز لهذه الصفحات أن بعضها على صلة مع دبلوماسيين وساسة بارزين من عدة دول أوروبية. لكن ليست هناك طريقة لمعرفة ما إذا كانت اتصالات أخرى جرت باستثناء الإضافة على موقع التواصل، ويعكس التحذير تنامي القلق في أجهزة المخابرات الأوروبية والغربية من أنشطة صينية سرية في بلادها ويأتي في أعقاب تحذير من وكالة المخابرات المركزية الأمريكية من محاولات أجهزة أمنية صينية تجنيد مواطنين أمريكيين للعمل لحسابها.

هجمات إلكترونية على منشآت للطاقة والطيران والمياه

أصدرت الإدارة الأمريكية تحذيرا نادرا للجمهور من شن حملات تسلل إلكتروني على مؤسسات للطاقة وأخرى صناعية في أحدث دليل على أن هذا النوع من الهجمات يشكل خطورة على صناعة

الطاقة وغيرها من البنى التحتية العامة، وأصدرت وزارة الأمن الداخلي ومكتب التحقيقات الاتحادي (إفببآي) الأمريكي تقريراً نشر عبر رسائل البريد الإلكتروني مساء الجمعة ورد فيه أن منشآت صناعية في مجالات الطاقة النووية والطاقة والطيران والمياه وغيرها من الصناعات الحيوية، إضافة إلى جهات حكومية، تتعرض لهجمات تسلل إلكتروني منذ شهر مايو أيار على الأقل.

وحذرت الوزارة والمكتب من أن المشاركين في عمليات التسلل الإلكتروني نجحوا في التسلل إلى بعض الشبكات التي استهدفوها دون أن تحدد أي ضحايا أو تصف أي حالات للتخريب، وذكر التقرير أن هدف المهاجمين هو تعريض شبكات المؤسسات لرسائل بريد إلكتروني خبيثة للحصول على معلومات للوصول إلى شبكات الكمبيوتر المستهدفة.

وتعكف السلطات الأمريكية على مراقبة هذا النشاط منذ شهور وجاء ذلك في تقرير سري نشرته رويترز في يونيو حزيران. ووزع هذا التقرير على الشركات المعرضة لخطر الهجمات، ورفض سكوت ماكونيل المتحدث باسم وزارة الأمن الداخلي توضيح المعلومات التي تضمنها التقرير أو الدافع وراء إصدار الحكومة لهذا التحذير في هذا التوقيت، وقال "التحذير يوفر توصيات... للحد من أنشطة الإنترنت الخبيثة التي تستهدف قطاعات متعددة ويؤكد التزامنا باليقظة في مواجهة (أي) تهديدات جديدة"، ولم يرد ممثلون لمكتب التحقيقات الاتحادي على طلبات للتعليق، وقال التقرير إن وزارة الأمن الداخلي "على ثقة بأن هذه الحملة لا تزال مستمرة ولا يزال ممثلو التهديد يسعون نحو (تحقيق) أهدافهم في حملة طويلة المدى".

تقارير: متسللون روس سرقوا أسراراً إلكترونية من وكالة الأمن القومي الأمريكي

قالت صحيفتان أمريكيتان إن متسللين مدعومين من الحكومة الروسية سرقوا معلومات إلكترونية أمريكية شديدة السرية من وكالة الأمن القومي عام 2015 بعد أن وضعها أحد المتعاقدين على جهاز كمبيوتر في منزله.

ونقلت صحيفة وول ستريت جورنال عن مصادر لم تسمحها قولها إن السرقة تضمنت معلومات بشأن اختراق شبكات الكمبيوتر الأجنبية والحماية من الهجمات الإلكترونية، ورجحت أن تكون هذه من

أكبر الاختراقات الأمنية على الإطلاق.

وجاء في خبر نشرته صحيفة واشنطن بوست لاحقا أن الموظف عمل مع وكالة الأمن القومي قبل طرده منها عام 2015، وامتنعت وكالة الأمن القومي عن التعليق مشيرة إلى سياسة "عدم التعليق نهائيا على القضايا التي تخص منشآتها أو موظفيها". ولم يتسن لرويترز التحقق بشكل مستقل من التقارير.

وإذا تأكد النبأ فسيكون هذا أحدث اختراق في سلسلة اختراقات لبيانات سرية تخص وكالة الأمن القومي الأمريكية ومنها تسريب المتعاقد إدوارد سنودن بيانات سرية بشأن برامج المراقبة الأمريكية عام 2013، وينتظر متعاقد آخر يدعى هارولد مارتن محاكمته في اتهامات بأخذ مواد سرية تابعة لوكالة الأمن القومي الأمريكية إلى منزله. وقالت واشنطن بوست إن مارتن لم يلعب دورا في القضية الأخيرة.

وقال السناتور بن ساس عضو لجنة الخدمات المسلحة بمجلس الشيوخ في بيان ردا على تقرير وول ستريت جورنال إن التفاصيل تنذر بالخطر إذا كان ما ورد في التقرير صحيحا، وأضاف "يجب أن ترفع وكالة الأمن القومي رأسها من الرمال وتحل مشكلة متعاقدتها"، ونقلت الصحيفتان الأمريكيتان عن مصادر لم تسمها قولها إن المتعاقد استخدم برنامج مضاد للفيروسات من شركة كاسبرسكي وهي شركة مقرها موسكو تقرر الشهر الماضي حظر استخدام منتجاتها داخل شبكات الحكومة الأمريكية للاشتباه بأنها تساعد الكرمليين على عمليات التجسس، ونفت الشركة تلك المزاعم بشدة، وقال خبراء أمنيون إن مسؤولي الحكومة الروسية استغلوا ثغرات في برنامج كاسبرسكي لاختراق جهاز المتعاقد، وقالت كاسبرسكي أمس الخميس إنها وجدت نفسها في خضم عراك سياسي.

برنامج كاسبرسكي استخدم لاختراق كمبيوتر متعاقد مع وكالة الامن القومي الاميركية

أوردت صحيفة وول ستريت جورنال ان قرصنة معلوماتية روس استخدموا برنامج "كاسبرسكي" المضاد للفيروسات الإلكترونية لسرقة وثائق سرية كانت على جهاز الكمبيوتر الشخصي لمتعاقد مع

وكالة الامن القومي الاميركية في 2015، وتابعت الصحيفة الخميس ان القرصنة تمكنوا بذلك من الوصول الى وثائق تشرح كيف تقوم "الوكالة بقرصنة أجهزة كمبيوتر أجنبية وكيف تحمي نفسها من عمليات القرصنة.

وعملية القرصنة التي تمت في العام 2015 كانت الثالثة التي يتعرض لها متعاقد مع الوكالة في غضون اربع سنوات. ولعل الحادث حمل السلطات الاميركية على منع الوكالات الفدرالية من استخدام هذا البرنامج الذي تطوره شركة "كاسبرسكي لابس" المتخصصة في الامن المعلوماتي، في 13 ايلول/سبتمبر الماضي، أصدرت الحكومة الاميركية أمراً الى كل الوكالات الفدرالية بمسح برامج "كاسبرسكي" في غضون تسعين يوماً.

وكانت وزيرة الامن الداخلي ايلين ديوك أعلنت في بيان آنذاك ان "الوزارة قلقة من الروابط بين بعض المسؤولين في 'كاسبرسكي' وهيئات استخبارات ووكالات حكومية روسية أخرى"، وأوردت "وول ستريت جورنال" ان المتعاقد اخذ وثائق سرية تابعة لوكالة الأمن القومي الى منزله وقام بنسخها على جهازه الخاص الذي كن مزودا ببرنامج "كاسبرسكي". وتمكن القرصنة من تحديد الوثائق بفضل هذا البرنامج، وأضافت ان المتعاقد لم يكشف المعلومات عن قصد لكنه خالف القانون على الارجح عندما نقل وثائق مصنفة اسراراً دفاعية الى منزله.

من جهتها، شددت شركة "كاسبرسكي لابس" على عدم وجود دليل بحصول تواطؤ محتمل بينها وبين اجهزة الاستخبارات الروسية، وكتب مؤسس الشركة يوجين كاسبرسكي على مدونته "لنفترض ان شخصا او اثنين نجحوا بشكل أو بآخر في اختراق الشركة، هناك عشرات الآليات الداخلية والتكنولوجية وعلى مستوى التنظيم للحد من المخاطر"، كما انه سيتم كشف هؤلاء الاشخاص حتماً من قبل موظف آخر، وشدد كاسبرسكي على ان "استغلال ثقة مستخدمينا لتسهيل التجسس من قبل حكومة ما سيكون مخالفاً لمبادئنا الاخلاقية"، تحقق "كاسبرسكي لابس" 85% من مبيعاتها عبر الصادرات ويستخدم برنامجها لمكافحة الفيروسات ملايين الاشخاص في مختلف انحاء العالم.

مسؤول امني بريطاني يتهم روسيا بالتورط في هجمات معلوماتية على بريطانيا

من المتوقع ان يتهم مدير الامن المعلوماتي في بريطانيا روسيا بشن هجمات معلوماتية على وسائل اعلام بريطانية وعلى قطاعي الطاقة والاتصالات السنة الماضية، وسط تقارير عن تدخل روسي في الاستفتاء على خروج بريطانيا من الاتحاد الاوروبي (بريكست).

وبحسب مقتطفات من خطابه نشرها مكتبه مسبقا يقول كيران مارتن رئيس المركز الوطني للامن المعلوماتي ان "روسيا تسعى لتقويض النظام العالمي. هذا واضح"، ويضيف "التدخل الروسي الذي رصده المركز الوطني للامن المعلوماتي في السنة الماضية، تضمن هجمات على وسائل الاعلام في المملكة المتحدة وقطاعي الاتصالات والطاقة".

وسيقول ايضا "ان رئيسة الوزراء (تيريزا ماي) أكدت مساء الاثنين ان النظام العالمي كما نعرفه يواجه خطر الزوال"، وتفاعل المركز مع اكثر من 590 حادثة مهمة منذ إنشائه في 2016، رغم ان الوكالة الحكومية لم تحدد عدد تلك المرتبطة بروسيا، وتأتي تعليقات مارتن بعد هجمات لاذعة من ماي لروسيا التي اتهمتها "بالسعي لاستخدام المعلومات كسلاح" و"بنشر الخلافات في الغرب وتقويض مؤسساتنا".

وقالت الاثنين في كلمة خلال المأدبة الرسمية لبلدية لندن ان النشاطات الالكترونية الروسية تشمل "استخدام منظماتها الاعلامية الحكومية لزرع روايات كاذبة ونشر صور تم التلاعب بها"، ورفضت وزارة الخارجية الروسية الانتقادات واتهمت ماي بتحويل انتباه الشعب عن المشكلات الداخلية، والمحاولات الروسية المفترضة للتأثير على استفتاء بريكست العام الماضي، هي ضمن تحقيق يجري في لندن، وقد طلبت اللجنة البرلمانية للمعلومات الرقمية والثقافة ووسائل الاعلام والرياضة معلومات من تويتر وفيسبوك عن حسابات مرتبطة بروسيا، وتسعى هذه اللجنة للاستماع الى مدراء تنفيذيين من مواقع التواصل الاجتماعي في السفارة البريطانية في واشنطن مطلع العام القادم.

أرباح شركات عالمية تتضرر من هجمات إلكترونية

تضررت أرباح شركات جراء هجمات إلكترونية مكلفة تزيد أثرها وأصبحت أمرا واقعا لشركات مثل مونديليز المنتجة لبسكويت أوريو وميرك للأدوية وغيرهما ممن قالوا إن هجوما وقع في

الأسفوع الأففر من الربف الثاني عطل بعض العمليات.

وسجلت موندلفز انترناشونال، ثاني أكبر شركة حلوفات فف العالم، انخفاضا بلغ خمسة فف المئة فف المففعات الفصففة فف النئافج الفف أعلنتها ففم الأربعاء عزته إلى تأخفرات النقل البفرى والفواففر بفعل الهجوم الإلكتروني المعروف باسم "نوت بفففا" فف 27 ففونفو حزفران، وكان من بفن ضحافا نوت بفففا الآخرفن مفرك الفف حذرت الأسفوع الماضي من أن الهجوم تسبب فف وقف إنئافج بعض الأفوفة وقالئ إنها لم تقدر بعد الفكلفة الإجمالفة المرئبطة بالهجوم، وتسبب الهجوم أيضا فف -ئباطؤ عمليات التسلفم لءى ففءفكس وتعطفل عمليات موائئ لشركة النقل البفرى إففبف موفر مفرسك وئوقف خطوط إنئافج لءى رفكفئ بفنكفسر البرفطائفة المنئجة للسلف الاستهلافكة وففا لئلك الشركات.

وقال أففان وفنر الرئفس المشارك للأسهم لءى وفءبوش للأوراق المالفة "فجب أن ففئاء المسئثمرون على سماع ما فئعلق بهجمات إلكئرونفة خلال إعلناف الأرباف، "هذا الآئافه فئسارع.. مع اسئءامهم أسالفب أكثر تعقفا، ففهاجم القراصنة شركات كبفرة"، وأصبف الكئفر من القراصنة معئاففن على ئطوفر برمففات فبفئة لمحو البفاناف المسجلة على أجهزة الكمبفوتر وجعلها فر صالحة للعمل.

فبراء أمن: إفران طورت قدراتها فف التسلل الإلكتروني بعد أن كانت مئئءة

قالئ مؤسسة فافر آف الأمففة الأمريكية إن مئسلفن مرئبئفن على الأرجف بالحكومة الإفرانفة مسؤولون عن هجمات إلكئرونفة على شركات سعودفة وفربفة فف مجالف الطفران والفضاء والبئروكفماوفاف فف مؤشر على ئطور القدرات الإفرانفة على الآئراق الإلكتروني، وأطلق ئقفرر للشركة على المئسلفن الجءء اسم مموعة إففبفئف 33 وئءء بالفصفل عن أدلة على أنشئة المموعة منذ 2013 فف السعف للاسئلاء على أسرار عسكرفة وجوءة مع الاسئءاء لشن هجمات ربما ئفضف إلى انهفار شبكات كمبفوتر بأكملها.

ولم فئسن الوصول بعد لقواف الحرس الثورف الإفرانف للئعقفب بعد أن ائصلئ بها روفئرز فف نهاية أسفوع العمل فف البلاد، ورصدئ الشركة مموعة إففبفئف 33 بعد أن اسئءعئ لإجراء ئقففات

في هجمات إلكترونية على منظمة أمريكية للطيران ومجموعة شركات سعودية تملك حصصا في شركات طيران ومجموعة كورية جنوبية لها مصالح في مجال تكرير النفط والبتروكيماويات. ورفضت فاير آي ذكر أسماء هذه الشركات.

وفي تحرك منفصل الأسبوع الماضي أدرجت وزارة الخزانة الأمريكية شبكتي تسلل تتخذان من إيران قاعدة لهما وثمانية أفراد في قائمة للعقوبات الأمريكية متهمة إياهم بالمشاركة في هجمات إلكترونية على النظام المالي الأمريكي.

وقالت فاير آي إن مجموعة إيهبيتتي33 كانت أول مجموعة تدعمها الدولة من إيران تنضم إلى قائمة جمعتها الشركة خلال العقد الأخير وتشمل حملات لمتسللين إلكترونيين من الصين وروسيا وكوريا الشمالية، وقال جون هولتكويست مدير تحليل بيانات التجسس الإلكتروني في الشركة لرويترز في مقابلة "هذه الحملة تحمل بصمات الإيرانيين لاسيما بصمات الحكومة. في اللحظة الراهنة نشهد الكثير من الأنشطة التي يبدو أنها تجسس إلكتروني تقليدي".

وذكر هولتكويست أن مجموعة إيهبيتتي33 تشترك في بعض الأدوات مع 15 مجموعة تسلل لها صلات بإيران لكنها تختلف عنها في الوقت ذاته. ورصد باحثون في مجال الأمن هذه المجموعات في السنوات الأخيرة ويحمل بعضها أسماء مثل "شامون" و"وروكيت كيتن" و"تشارمينج كيتن"، ويقول بعض الخبراء إن استخدام كلمة "كيتن" أو الهريرة في الإشارة لهذه المجموعات يعكس درجة الاعتداد بقدرات إيران في الماضي، وذكرت فاير آي أن الهجمات ضد المجموعتين السعوديتين والكورية الجنوبية حدثت في فترة قريبة أحدثها كان في مايو أيار الماضي واستخدمت أساليب التصيد لسرقة بيانات حسابات البريد الإلكتروني والتي تتضمن رسائل مزيفة عن إعلانات وظائف في شركات نفط في السعودية لاجتذاب الضحايا.

باحثان يكشفان خلايا جعل الإنترنت اللاسلكي عرضة للاختراق

حذرت وزارة الأمن الداخلي الأمريكية من مخاطر إلكترونية مرتبطة بنظام مستخدم على نطاق واسع لتأمين الاتصالات عبر الإنترنت اللاسلكي (واي-فاي) بعد أن اكتشف باحثان بلجيكيان خلايا قد

يتيح لمتسللين قراءة معلومات كان يعتقد أنها مشفرة أو إصابة المواقع بالبرمجيات الخبيثة، وجاء في التحذير الذي أصدره فريق الاستجابة للطوارئ المتعلقة بأجهزة الكمبيوتر التابع لوزارة الأمن الداخلي أن الخل يمكن استغلاله ضمن نطاق شبكة الإنترنت اللاسلكي باستخدام بروتوكول التشفير (دبليو.بي.إيه2) لاختراق اتصالات خاصة. وأوصى الفريق بتحديث المنتجات المتأثرة بهذا الخل مثل أجهزة التوجيه التي تقدمها شركة سيسكو سيستمز أو جونيبر نتووركس، وكشف الباحثان البلجيكيان ماثي فانهورف وفرانك بيسنز من جامعة كو لوفن البلجيكية الخل في بروتوكول التشفير (دبليو.بي.إيه2) الذي يؤمن أنظمة الإنترنت اللاسلكي الحديثة والذي يستخدمه الباعة للاتصالات اللاسلكية بين أجهزة الهواتف المحمولة والكمبيوتر المحمول وغيرها من الأجهزة المتصلة بأجهزة توجيه متصلة بالإنترنت أو بشبكات إنترنت لاسلكية.

قال الباحثان "إذا كان جهازك يدعم الاتصال بالإنترنت لاسلكيا فإنه تأثر على الأرجح". وكتب الباحثان نتائجهما على موقع كراك أتاكس الذي أسسها لتقديم المعلومات التقنية عن الخل والأساليب التي قد يستخدمها المتسللون لمهاجمة الأجهزة، ولم يتضح على الفور مدى صعوبة استغلال المتسللين للخل أو إن كان الخل استخدم من قبل لشن هجوم.

جوجل تدشن خصائص متقدمة لحماية البريد الإلكتروني للمستخدمين المعرضين للخطر

قالت شركة جوجل إنها ستطرح "برنامج حماية متقدما" لتوفير أمن أقوى لحسابات البريد الإلكتروني لبعض المستخدمين مثل مسؤولي الحكومة والنشطاء السياسيين والصحفيين المعرضين بدرجة أكبر لخطر الاستهداف من متسللين متطورين، وسيتاح لمستخدمي جوجل اختيار إعدادات أمن تهدف لحماية بيانات بريد جوجل الإلكتروني (جيميل) وقاعدة تخزين البيانات (جوجل درايف) ويوتيوب من هجمات التصيد الإلكتروني.

وتتضمن خصائص الحماية المتقدمة خيارا يتطلب مفتاحا آمنا في هيئة جهاز ناقل للبيانات يتم توصيله بجهاز الكمبيوتر قبل أي محاولة لدخول الحسابات للتحقق من هوية المستخدم. وستتطلب محاولات الدخول للحسابات عن طريق الهواتف المحمولة جهازا لاسلكيا يعمل بالبلوتوث، وسيتم

منع تطبيقات من أطراف آالثة مثل خدمة البريد الإلكتروني لأبل أو برنامج مايكروسوفت أو تلوكن من الوصول لبيانات المستخدمين الذين سيتمتعون بخصائص الحماية المتقدمة، ويتضمن البرنامج أيضا عملية معقدة ومفصلة لاستعادة الحسابات لقطع الطريق على المتسللين الذين يحاولون الوصول لحسابات عن طريق التظاهر بأنهم مستخدمون فقدوا حساباتهم.