# نيويورك تايمز: قراصنة معلوماتية حاولوا إحداث انفجار في مصنع سعودي

"خطر كبير"، هذا ما تحدثت عنه صحيفة "نيويورك تايمز"، خلال رصدها لهجوم تخريبي استهدف السعودية الفترة الماضية.

وقالت الصحيفة الأمريكية إن شركة بتروكيماويات في السعودية تعرضت في أغسطس/ آب الماضي، لنوع جديد من الهجمات الإلكترونية، وصفه الخبراء بأنه يشكل خطرا كبيرا.

ونقلت عن باحثين قولهم إن خطورة ذلك الهجوم الإلكتروني في أنه لم يكن يستهدف تدمير البيانات أو إغلاق المصنع، ولكنه كان يستهدف "تخريب عمليات الشركة"، وربما "إحداث انفجار فيها".

ووصفت "نيويورك تايمز" الهجوم بأنه تصعيد خطير في الحرب الإلكترونية العالمية، وأظهرت أن الأعداء الذين لم تكشف هويتهم، يمتلكون القدرة على إلحاق "أضرار مادية" خطيرة.

ويخشى مسؤولون في الولايات المتحدة وعدد من الدول الغربية والباحثون في مجال الأمن الإلكتروني، بحسب الصحيفة الأمريكية من أن يكرر الجناة مثل تلك الهجمات في بلدان أخرى، يوجد بها آلاف من المناطق الصناعية، التي تعتمد على نفس أنظمة الأمان الحاسوبية الأمريكية، التي تم اختراقها.

ولم يحدد المحققون حول هجوم أغسطس، حتى الآن الشركة أو البلد، مصدر الهجوم.

وكانت صحيفة "الوطن" السعودية قد تحدثت عن الهجوم الإلكتروني، وأشارت إلى أن الهجمات استهدفت عدة مواقع في المملكة، وأدت إلى تعطيل أنظمة العمل الإلكترونية في 3 مصانع بتروكيماويات في منطقة "الجبيل"، وهم شركات "صدارة، والتصنيع، والمتقدمة"، فيما نجت الشركة الرابعة، وهي "سبيكم"، بعدما علق المسؤولون نظام التشغيل الإلكتروني للمصنع.

واستمرت "نيويورك تايمز" في الحديث عن طبيعة الهجوم الإلكتروني، ووصفت المهاجمين بأنهم كانوا "أكثر تطورا" ويمتلكون أدوات وموارد متفوقة.

ونقلت الصحيفة عن أكثر من 12 خبيرا في الأمن الإلكتروني، طلبوا عدم الكشف عن هويتهم لمشاركتهم في التحقيقات السرية، قولهم إن التطور والتقدم في هذا الهجوم يوحي بأنهم على الأرجح كانوا مدعومين من قبل حكومة ما.

وأشار المحققون إلى أن الشيء الوحيد، الذي حال دون وقوع الانفجار، هو خطأ في أكواد الحواسب الخاصة

بالمهاجمين.

ويعتقد المحللون أن المتسللين، ربما قاموا بتحديد خطأهم حاليا، ولن يكون الأمر إلا مسألة وقت فقط، ليتمكنوا من العثور على طريقة جديدة لاختراق نظام التحكم الصناعي أكثر فعالية بالنسبة لهم.

وأوضحت الصحيفة أن "الهجوم الأكثر إثارة قلقا في سلسلة من الهجمات الإلكترونية على مصانع البتروكيماويات في السعودية، الذي تم في يناير/كانون الثاني 2017ن والذي أدى لتعطيل أجهزة الكمبيوتر لشركة التصنيع الوطنية، والذي يبعد 15 ميلا عن شركة صدارة للكيماويات، وهو مشروع مشترك بين شركة آرامكو السعودية وشركة داو كيميكال".

وأردفت "في غضون دقائق من هذا الهجوم، تم تدمير كافة محركات الأقراص الصلبة لأجهزة الكمبيوتر الخاصة بالشركة، وتم محو جميع بياناتها، واستعيض بدلا منها بصورة الطفل السوري الصغير، آلان كردي، الذي غرق قبالة السواحل التركية".

وقال مسؤولو في شركة "تاسنيي" وباحثون في شركة "سيمانتيك" المتخصصة في أمن المعلومات: "الهدف من الهجوم إلحاق الضرر الدائم بشركات البتروكيماويات، وتوجيه رسالة سياسية قوية".

وقالت إيمي مايرز جافي، الخبيرة في شؤون الطاقة في الشرق الأوسط بمجلس العلاقات الخارجية: "ليس فقط هجوم على القطاع الخاص، بل هجوم كان يسعى لإيقاف النمو في الاقتصاد السعودي، الذي كان يركز بصورة خاصة على قطاع البتروكيماويات".

وأشارت إلى أنه لا يزال محللو أمن في شركة "مانديانت"، وهي شركة تابعة لشركة "فاير آيي" لأمن المعلومات، في هجوم أغسطس، بمساعدة عدد شركات أمريكية، تراجع أنظمة المراقبة الصناعية بالكامل.

كما قال أشخاص ضمن فريق بشركة "شنايدر إلكتريك" المتخصصة في تصنيع الأنظمة الصناعية المستهدفة، وأن تلك الأنظمة يطلق عليها "تراكونيكس"، وأوضحت أنه يشارك في التحقيقات وكالة الأمن القومي الأمريكي والمباحث الفيدرالية الأمريكية ووزارة الأمن الداخلي الأمريكي ووكالة مشاريع الأبحاث المتقدمة الدفاعية التابعة لوزارة الدفاع.

وظهر فيروس "شمعون"، الذي أثار قلقا كبيرا في السعودية أيضا لأول مرة قبل 5 سنوات، عندما استهدف شركة "أرامكو" السعودية، وهو ما جعل وزير الدفاع الأمريكي حينها، ليون بانيتا، للتحذير من أن "الهجوم قد يكون نذيرا".

وقال بانيتا: "يمكن لأي أمة معتدية أو لجماعة متطرفة استخدام هذه الأنواع من الأدوات السيبرانية للسيطرة على المفاتيح الحساسة".

ونسب مسؤولون حكوميون وخبراء في الأمن الإلكتروني في السعودية والولايات المتحدثة، نسبوا هجوم فيروس شمعون عام 2012 إلى قراصنة إيرانيون.

وقال فيكرام تاكور، أحد كبار الباحثين في سيمانتيك: "كان من الممكن أن يتبنى مهاجم آخر مختلف عن هجوم يناير 2017، لكن كافة الاحتمالات تشير إلى أنه قد يكون الجاني نفسه".

ويعتقد محققون أن شخصا ما يمكن أن يكون قد اشترى نسخة من نظام أمان "تراكونيكس" لمعرفة كيفية عمله، وأوضحوا أنه يمكن شراء كافة مكوناته مقابل 40 ألف دولار من على موقع تجارة إلكتروني.

وقال خبراء في الأمن السيبراني إن إيران والصين وروسيا والولايات المتحدة وإسرائيل، يمتلكون التطور التقني لشن مثل هذه الهجمات.

وتنفي الحكومة الإيرانية أي تورط لها في أي هجمات إلكترونية، مرارا وتكرارا.

وقال خبير في شركة "سيمانتك" إن "هجوم أغسطس أكثر تطورا بكثير من أي هجوم سابق نشأن من إيران، ولو كانت هي، فإذن طهران تمكنت من تحسين قدراتها في مجال الحرب السيبرانية بصورة كبيرة بالعمل مع دولة أخرى".

وردت وكالة أنباء "تسنيم" الإيرانية في رسالة عبر البريد الإلكتروني لصحيفة "نيويورك تايمز" قائلة "إن خبراء من سيمانتك وآي بي إم، استعانت بهم طهران لدراسة الهجوم الواقع ضدها".

وأوضحت الوكالة الإيرانية أن الخبراء أصلحوا معايير الأمان الخاصة بأجهزة الإيرانية، واستخدموا أدوات جديدة لمنع أي هجمات إلكترونية. (سبوتنيك)