تفاصيل الهجوم.. قراصنة يدمرون كومبيوترات في وكالة الطيران السعودي..

ويستبدلون البيانات بصورة الطفل السوري آلان كردي.. وتوجيه أصابع الاتهام لايران

دبي ـ وكالات: دمر قراصنة إلكترونيون كومبيوترات في ست منشآت سعودية مهمة قبل أسبوعين، ما يشكل عودة ظهور للسلاح الإلكتروني الأكثر ضرراً الذي شهده العالم على الإطلاق.

وقالت السعودية ان دوائر رسمية "متعددة" كانت هدف هجمات من خارج المملكة، ورغم ان التحقيق الذي بدأته السلطات السعودية ما زال في مراحله المبكرة فان مصادر قالت لشبكة بلومبرغ نيوز ان الأدلة الرقمية تشير الى ان الهجمات انطلقت من ايران ، وان هذا يمكن ان يطرح على الرئيس الاميركي المنتخب دونالد ترامب تحدياً أمنياً كبيراً حين ينتقل الى البيت الأبيض.

آخر مرة، استُخدمت القرصنة في عام 2012، لتدمير 35 ألف جهاز كمبيوتر في شركة النفط السعودية "أرامكو،" وألقت المخابرات الأمريكية اللوم بهدوء على إيران عن ذلك الهجوم.

هذه المرة، هاجم القراصنة وكالة حكومية سعودية واحدة على الأقل، بالإضافة إلى منظمات في قطاعات الطاقة والصناعة والنقل، وفقا لاثنين من الباحثين على إطلاع مباشر بالتحقيقات في الهجوم.

ويتجه الباحثون في مجال الأمن الآن إلى المملكة العربية السعودية لمعرفة كيف محى القراصنة البيانات على أجهزة الكمبيوتر بشكل جماعي، وفقا لعدد من الخبراء المعنيين.

وأكدت وكالة الأنباء السعودية "واس"، الخميس، وقوع هجوم إلكتروني "على مختلف المؤسسات الحكومية والهيئات."

وأضاف التقرير الرسمي أن "الهجمات استهدفت تعطيل جميع الخوادم والأجهزة بحيث يؤثر ذلك على جميع

الخدمات المقدمة،" وأن المهاجمين استولوا على بيانات الأنظمة الحاسوبية وزرعوا البرمجيات الخبيثة.

واستهدف القراصنة الهيئة العامة للطيران المدني التي تنظم الطيران السعودي، وفقا لباتريك واردل، وهو باحث في شركة الأمن الإلكتروني "Synack". وقال إن أسلوب برمجة البرامج الخبيثة يُشير إلى استهداف موظفي هيئة الطيران المدني بشكل خاص.

وتعد الهجمات الإلكترونية المدمرة بهذا النطاق نادرة.

استخدم القراصنة نسخة من نوع معين من الأسلحة الإلكترونية، يُلقب بـ"شمعون"، والذي يعمل مثل قنبلة موقوتة.

العديد من شركات الأمن الإلكتروني الكبيرة، مثل "CrowdStrike" و"FireEye" و"McAfee" و"Alto Networks" و"Symantec"، أصدرت تقاريرا ً هذا الأسبوع توثق الهجوم فيها.

وفي التاسعة إلا ربع مساء ً بتوقيت السعودية، يوم 17 نوفمبر/ تشرين الثاني الماضي، بدأت البرمجيات الخبيثة بمحو البيانات المخزنة في أجهزة الكمبيوتر في المؤسسات السعودية. وتم استبدال جميع ملفات الكمبيوتر بصورة الطفل السوري اللاجئ، آلان الكردي، البالغ من العمر 3 سنوات، والذي عُثر على جسده على شاطئ تركيا مرميا ً بعد غرقه في طريق هربه من سوريا إلى أوروبا.

ثم سيطرت البرمجيات الخبيثة على سجل تمهيد أجهزة الكمبيوتر، ومنعت إعادة تشغيلها.

ولكن من السابق لأوانه إلقاء اللوم على دولة معينة أو منظمة إجرامية أو مجموعة قراصنة سياسية (hacktivists).

وأشار أحد مؤسسي شركة "CrowdStrike"، ديميتري ألبيروفيتش، إلى أن الاختراق حدث قبل أيام فقط من موافقة دول "أوبك" خفض إنتاج النفط للمرة الأولى منذ 8 سنوات. ويلعب الاتفاق في صالح إيران، إذ يسمح لها برفع مستويات إنتاجها لتصل للمستويات التي كانت تضخها قبل فرض العقوبات الاقتصادية عليها؟

وقال كولين أندرسون، أحد كبار الخبراء في العالم في نشاط القرصنة الإيراني، إنه يحتمل استخدام إيران هذا الهجوم للضغط على المملكة العربية السعودية.

إذ أضاف أندرسون، الذي يعمل على بحث لمؤسسة "كارنيغي" للسلام الدولي، يتتبع فيه تاريخ الحرب الإلكترونية الإيرانية: "لقد شهدنا ارتفاعا ً كبيرا ً في مستوى نشاط التجسس الذي تقوم به مجموعات القراصنة المرتبطة بالحكومة الإيرانية."

واتبع هذا الهجوم الأخير الذي استخدم "شمعون،" نمطا ً مماثلا ً لهجوم مدمر سابق على شركة "أرامكو" السعودية في عام 2012.

ويقول إريك شين، المدير الفني في شركة "Symantec"، إنه من الملفت للنظر أن المتسللين استخدموا ذات السلاح الإلكتروني ضد هدف سعودي آخر، وأن الهجوم نجح.