للمرة الثالثة.. "شمعون" يهاجم السعودية

خاص – التقرير

مرة أخرى ضرب فيروس "شمعون"، مؤسسات سعودية منها وزارات العمل والتنمية الاجتماعية والاتصالات وتقنية المعلومات والنقل، وغيرها من مؤسسات غير حكومية.

وكانت هيئة الاتصالات وتقنية المعلومات ممثلة في المركز الوطني الإرشادي لأمن المعلومات حذرت من هجمات إلكترونية مختلفة من نوع فيروس "شمعون2"، وفيروس الفيدية يستهدفان المعلومات والملفات وتمسحها كاملة، وأوصت جميع الجهات برفع مستوى الحيطة والحذر والتحقق من وجود الاحتياطات اللازمة. وجاء تحذير هيئة الاتصالات بعد تعرض عدد من الجهات الحكومية والوزارات لهجمات أدت لعطل في أنظمتها الداخلية، وأوصت ببعض الحلول المقترحة التي قد تساعد في تفادي الإصابة وتقليل الأضرار.

وزارة العمل

وأوضح المتحدث الرسمي لوزارة العمل والتنمية الاجتماعية خالد أبا الخيل، أن الوزارة وصندوق تنمية الموارد البشرية (هدف)، تعرضتا لهجوم إلكتروني بواسطة فيروس، وجرى التنسيق مع المركز الوطني للأمن الإلكتروني في وزارة الداخلية، باحتواء انتشار الفيروس، فيما اتخذت الوزارة و"هدف" الاحتياطات المعلوماتية كافة، للتأكد من سلامة أنظمتهما، وعدم وجود أي أضرار قد تنتج على خلفية ذلك.

وقال المتحدث الرسمي للوزارة إن الوزارة و"هدف" اتبعتا التدابير اللازمة والإجراءات التقنية لحماية جميع قواعد البيانات، مؤكدًا أن الوزارة و"هدف" تمكنتا بعد تلقيهما البلاغات بالتعاون مع مركز

الأمن الإلكتروني من التعامل مع الفيروس، والحد من انتشاره وتوسعه.

موبايلي

أكدت "موبايلي" في بيان رسمي، تمكنها من تأمين وحماية جميع أنظمة الشركة نتيجة التقنية المتطورة والبنى التحتية المُطبقة لديها، إثر تعرضها لهجمات إلكترونية.

وأشار بيان "موبايلي" إلى تعرضها للهجمات الإلكترونية مثل شركات وقطاعات أخرى بالمملكة والمنطقة، وكانت شركة صدارة أعلنت أنها ضمن المؤسسات التي تعرضت لهجمات قرصنة من قبل فيروس "شمعون 2".

ماذا يفعل؟

ويعد فيروس شمعون أحد أكثر الأسماء المرعبة للأجهزة الحاسوبية، حيث لم يعرف من مطوره الحقيقي، وهو فيروس من النوع الخطير للغاية لاستهدافه كبريات الشركات حول العالم.

وفيروس شمعون، يستخدم في الهجمات الإلكترونية المنظمة ويسبب عطلاً للآلاف من الأجهزة. وتكمن خطورته في محو سجلات الإقلاع الرئيسية المهمة في بدء العمل.

هجوم سابق

وكان فيروس شمعون هاجم من قبل شركات عالمية في أمريكا وأوروبا ما استدعى خبراء تكنولوجيا المعلومات لإطلاق صيحات الحذر والاحتراس وتجنب فتح الرسائل المجهولة لتجنب الإصابة بهذا الفيروس الخطير.

ودخل فيروس مدمّر إلى عشرات آلاف من الكمبيوتر في الشرق الأوسط في العام 2012.

سبق لفايروس شمعون محاولة تدمير بيانات المملكة إلكترونيا، ففي 15 أغسطس من العام 2012 هاجم "شمعون" أجهزة كمبيوتر شركة الطاقة السعودية (أرامكو) نتج عنه تعطل 30 ألف حاسوب شخصي.

وفي 19 نوفمبر 2016، استهدف تعطيل الخدمات لبعض الجهات الحكومية، ومنشآت حيوية من بينها قطاع النقل.

وفي 23 يناير الجاري عمل على تعطيل موقع وزارة العمل والاتصالات وتقنية المعلومات وشركة صدارة للكيميائيات.

من وراء الهجمات؟

وجهت شركة سيمانتيك أصابع الاتهام إلى مجموعة قرصنة وتجسس إلكتروني تدعى "جرين بج" والتي تعتقد سيمانتيك أنها الجهة التي تقف وراء فيروس "شمعون" الذي عاد ليضرب في الساعات الماضية عددا من الجهات الرسمية في المملكة العربية السعودية. واستندت سيمانتيك في اتهامها على تحليل تقني معمق.

وكانت سيمانتيك اكتشفت مجموعة القرصنة والتجسس الإلكتروني "جرين بج" في أثناء تحقيقها في هجوم تسبب في تدمير ومسح بيانات استخدم فيه فيروس المعروف باسم شمعون.

ونشطت مجموعة القرصنة والتجسس "جرين بج" في شهر يونيو 2016، وتعتمد المجموعة في هجماتها على البريد الإلكتروني لتتمكن من اختراق المؤسسة.

وترى سيمانتيك، أن هذه المجموعة تملك صلاحيات دخول حصرية على البرمجية الخبيثة.

بينما الناطق باسم شركة "فاير آي" للحماية الإلكترونية أشار إلى أن المهاجمين جمعوا سابقا تسجيلات الدخول وكلمات السر اللازمة قبل دمجها في وقت لاحق في البرمجيات الخبيثة لشن هجوم مدمر.

كما أفاد بأن هجمات 2012 أجريت من قبل قراصنة يعملون لدى الحكومة الإيرانية إلا أنه لم يؤكد أن الطرف نفسه هو وراء شمعون 2.

فقد أعلن يوم 6 ديسمبر 2016، أنه في عام 2012، قامت عصابة مريبة من القراصنة الإيرانيين الذين أطلقوا على أنفسهم اسم "سيف العدالة القاطع" باستخدام برمجية خبيثة عرفت باسم "شمعون لاستهداف شركات الطاقة في منطقة الشرق الأوسط.

وأوضحت "فاير آي" أن الإصدار الثاني لفيروس شمعون هي نسخة معدلة ومحدثة من البرمجية الخبيثة التي شهدت في حادثة عام 2012. وتظهر التحليلات أن هذه البرمجية الخبيثة تحوي داخلها بيانات تعريف خاصة بتسجيل الدخول، ما يشير إلى احتمال قيام المهاجمين في السابق بعمليات اختراق موجهة للسطو على بيانات التعريف اللازمة قبل شن أي هجوم لاحق.