مما يعني كم هي فاشلة البنية التحتية في المجال المعلوماتي بعد أقل من شهرين فقط شمعون2 ينجح في الاختراق



عاود فيروس «شمعون2» مهاجمة جهات حكومية وحيوية في المملكة العربية السعودية عبر ملف مرفق، زرع بداخله برمجية خبيثة، تهدف إلى سرقة المعلومات، وذلك بعد أقل من شهرين على استهدافه أجهزة أكثر من 20 جهة حكومية وخاصة.

وأعلن مركز الأمن الإلكتروني التابع لوزارة الداخلية، عبر حسابه في «تويتر»، أمس السبت، رصد رسائل بريد تصيدية استهدفت جهات حكومية وحيوية، الخميس الماضي، مؤكدا إنذار الجهات المستهدفة وإرسال التوصيات لمنع حدوث الضرر.

وطالب المركز الجهات المستهدفة بتزويده بريديا بالبيانات اللازمة للحصول على المزيد من المعلومات.

من جهته، قال عضو الأكاديمية الأمريكية للطب الشرعي - الأدلة الرقمية الدكتور «عبدالرزاق المرجان»: «إن التحقيق لا زال في مراحله الأولية ويحتاج لوقت لمعرفة هل هو (شمعون2)

الإصدار الثاني أم تم تطويره، ما يعني استحداث بصمة جديدة لا تستطيع برامج الحماية التعرف عليها وهذا يصعب طرق اكتشافه تقنيا ويرجح الاختراق، وإن كان تم تطويره فهو يرجح احتمالية ما ذكرنا سابقا بأن هذه الهجمات تمول من دولة وهي في العادة إيران لحاجتها لمطورين مميزين على مستوى العالم».

وأضاف: «الطريقة المستخدمة لتفعيل الفيروس هي الطريقة ذاتها، وهي التقليدية الهندسة الاجتماعية ثم التصيد الإلكتروني، ونحن بحاجة إلى تدريب الموظفين ورفع الحس الأمني لدى المستخدمين في القطاع الحكومي لأنهم الحلقة الأضعف».

وتابع: «من المهم تحويل الموظفين إلى جدران حماية (جدار حماية بشري) Firewall Human حتى يكون الموظف هو خط الدفاع الأول في حالة التعامل مع التصيد الإلكتروني والهندسة الاجتماعية للإبلاغ عن البريد الإلكتروني المشبوهة».

وقد سجلت عدة حالات تم التعرف على «شمعون2» عن طريق موظفين حصلوا على تدريب يمكنهم من معرفة البريد الإلكتروني المشبوه بعد تجاوز «شمعون2» برامج الحماية لعدم تحديث برامج الحماية ببصمة «شمعون2» الإصدار الثاني، وتم إنقاذ جهة مهمة من الاختراق.

وحذر من نشر الشائعات عن الجهات المخترقة واستسقاء المعلومات من مصادرها، وعدم التشهير بالجهات الحكومية المتضررة لأسباب أمنية، مشيرا إلى أن أهداف هذه الهجمة سرقة المعلومات والتدمير الإلكتروني.

وظهرت النسخة الأولى من هذا الفيروس قبل نحو 4 أعوام، وهاجمت جهات حكومية، أهمها العملاق السعودي «أرامكو»، وخلفت خسائر مادية .

ويعطل الفيروس «شمعون» أجهزة الحاسوب من خلال استبدال برمجيات أساسية فيها، مما يجعل من المستحيل تشغيل الجهاز.