تقنيات كاسبرسكي لاب تكشف ثغرة في «ويندوز»

الخميس 11 أكتوبر 2018 08:10 م

كشفت شركة كاسبرسكى لاب للحلول الأمنية، عن سلسلة من الهجمات الإلكترونية الموجهة، استهدفت مستخدمين في منطقة في الشرق الأوسط

وجرت الهجمات باستخدام برمجية خبيثة جديدة استغلت ثغرة أمنية لم تكن معروفة من قبل في نظام التشغيل الشهير "ويندوز" من مايكروسوفت، وهدفت لتمكين المجرمين الإلكترونيين من الوصول الدائم إلى أنظمة الضحايا، وأغلقت مايكروسوفت الثغرة الأمنية 9 أكتوبر الجاري

ويُعد الهجوم من خلال الثغرات الأمنية المجهولة، والذي يُعرف باسم "هجوم بلا انتظار" أحد أخطر أشكال التهديدات الإلكترونية، نظراً لأنه ينطوي على استغلال ثغرة لم يتم اكتشافها أو إصلاحها بعد، ورغبة مجرمي الإنترنت بالمسارعة إلى استغلالها في شنّ هجمات قبل أن يتم إغلاقها، وإذا عثرت جهة تخريبية ما على ثغرة في نظام ما، فإنها تستطيع المسارعة إلى شنّ هجوم دون انتظار من أجل استغلال الثغرة والوصول إلى كامل النظام

ويستخدم هذا السيناريو على نطاق واسع من جهات تخريبية متطورة لشنّ هجمات متقدمة مستمرة، كما في الحالة التي تمّ اكتشافها

وقالت الشركة، فى بيان لها، أنه تم شنّ هجوم الاستغلال المكتشف في النظام "ويندوز" عن طريق المنفذ الخلفي PowerShell، قبل أن يتم تنفيذه من أجل الحصول على امتيازات الدخول اللازمة للبقاء على النظام الضحية، وقد كانت الشيفرة البرمجية الخبيثة عالية الجودة وتمت كتابتها لتتمكّن من عملية استغلال أكبر عدد ممكن من أنظمة "ويندوز".

واستهدفت الهجمات الإلكترونية أقل من اثني عشر شركة ومؤسسة في الشرق الأوسط خلال أواخر الصيف، ويُشتبه في أن الجهة التخريبية التي تقف وراء الهجوم يمكن أن تكون مرتبطة بمجموعة FruityArmor، إذ إن المنفذ الخلفي PowerShell المستخدم في الهجوم لم يُستخدم في الماضي إلاّ من قبل هذه العصابة التخريبية، وسارع خبراء كاسبرسكي لاب إلى إبلاغ مايكروسوفت عن هذه الثغرة عند اكتشافهم لها

وأكّد أنتون إيڤانوف الخبير الأمني لدى كاسبرسكي لاب، أهمية المراقبة الفعالة لمشهد التهديدات تحسباً لوقوع حوادث استغلال ثغرات مجهولة

وقال: "نهدف بسعينا المستمر في كاسبرسكي لاب للحصول على أحدث المستجدات والمعلومات المتعلقة بالتهديدات إلى العثور على هجمات جديدة، والتعرّف على الأهداف التي تسعى وراءها مختلف الجهات التخريبية الإلكترونية، فضلاً عن معرفة التقنيات الخبيثة التي يستخدمها هؤلاء المجرمون، وقد أصبحنا نمتلك أساساً متيناً من تقنيات الكشف التي تسمح لنا بمنع الهجمات، مثل تلك التي استهدفت استغلال ثغرة النظام ويندوز".