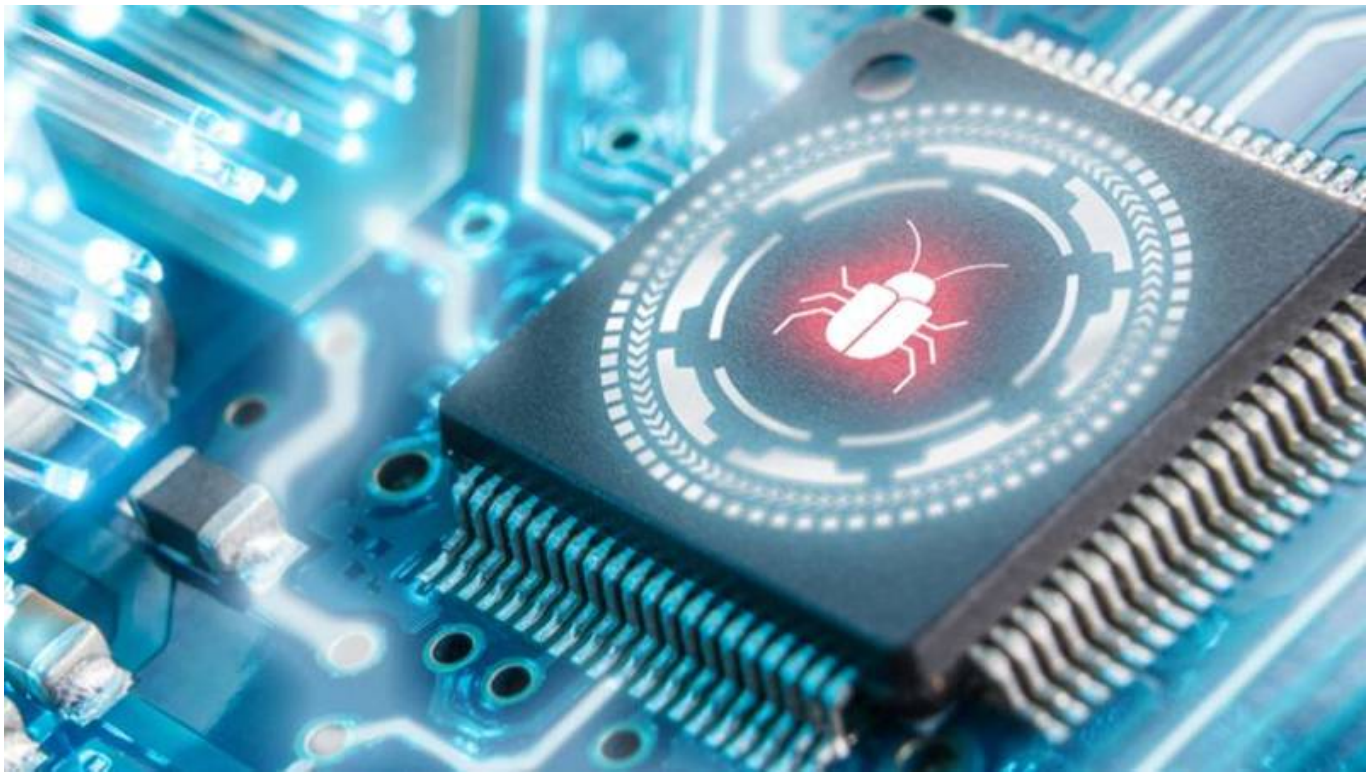
الخليج

اقتصاد, تقنية وسيارات

19 يونيو 2023 15:47 مساء

ارتفاع عمليات اكتشاف برنامج «روتكيت» المستهدفة الشركات 167 % الإماراتية



«دبي:«الخليج

ذكر خبراء كاسبرسكي ارتفاع عدد حالات اكتشاف برامج «روتكيت» التي تستهدف الشركات في الإمارات بنسبة 167% في الأشهر الخمسة الأولى من العام الجاري 2023. ويعني ذلك زيادة بمقدار 2.6 مرة عن الفترة ذاتها من العام 2022، كما يعكس هذا الارتفاع اتجاهاً مشابهاً في منطقة الشرق الأوسط التي توقعت ارتفاعاً مضاعفاً (103%) في عدد حالات اكتشاف الأدوات ذاتها، مقارنة بالأشهر الخمسة الأولى من العام الماضي

وتعتبر «روتكيت» برنامجاً خبيثاً أو مجموعة من البرامج التي يستخدمها المجرمون السيبرانيون للتجسس على جهاز كمبيوتر أو على شبكة معينة، بهدف الوصول إلى التحكم التام. وتتمثل إحدى أكثر الطرق انتشاراً التي يستخدمها هؤلاء المجرمون لتثبيت تلك الأدوات في تعريض سلسلة التوريد لضحية معينة للخطر. ويتميز هذا البرنامج بالقدرة على

التخفي، ويستخدم من قبل مجرمي الإنترنت لإخفاء وجودهم أثناء تنفيذ أنشطتهم الخبيثة وتجاوز الضوابط الأمنية. ويكون من الصعب في الكثير من الأحيان التحقيق في عمليات اكتشاف تلك الأدات وتحليلها. ونظراً لتصميمه المخادع للغاية، يستطيع المجرمون الاستيلاء على البيانات الشخصية، والوصول إلى المعلومات المالية، إضافة إلى تثبيت البرامج الخبيثة، واستخدام أجهزة الكمبيوتر كجزء من الروبوتات لتوزيع البريد العشوائي، أو لشن الهجمات الموزعة DDoS. لحجب الخدمة ويمتلك هذا البرامج الخبيث القدرة على التخفي داخل جهاز الكمبيوتر لفترة طويلة جداً، الأمر .الذي يتسبب في إحداث أضرار جسيمة

وقال عبدالصبور عروس، الباحث الأمني في فريق البحث والتحليل العالمي في كاسبرسكي: «تأتي مجموعات التهديدات المتقدمة المستمرة في صدارة مشهد التهديدات الإلكترونية، لاسيما وأنها تعتمد على»التخفي«، وتتخذه أساساً للتكتيكات الاستغلالية الناجحة، لاسيما وأنه يكون من الصعب على المستخدم حماية نفسه من شيء لا يمكن رؤيته. وتناسب هذه الأدوات تماماً نوع التقنية التي يستخدمونها. وكانت بعض مجموعات التهديدات المتقدمة المستمرة قد بدأت بتوظيف برامج»روتكيت«في أنشطتها، الأمر الذي جذب انتباه مجموعات التهديدات الأخرى ومجرمي الإنترنت وعصابات المتسللين. وأدى ذلك بمجمله إلى حدوث ما يطلق عليه بتأثير»الدومينو«، ومن ثم إلى زيادة استخدام تلك الأدوات ذاتها. ونظراً لإمكانية تثبيت البرنامج على أي أجهزة أو منصات برمجية، فقد أصبح الأمر .«أكثر خطورة، لاسيما وأن تقنيات إنترنت الأشياء والتقنيات القائمة على السحابة تخلق بيئة متكاملة ومتصلة جيداً