الخليج

اقتصاد, أسواق عالمية

27 يونيو 2021 15:27 مساء

بالو ألتو نتوركس»: 75% من الهجمات الإلكترونية على الشبكات خطرة»

دبي: «الخليج»

استعرضت شركة بالو ألتو نتوركس اليوك، أحدث التطورات التي تشهدها الهجمات الإلكترونية على الشبكات، حيث اكتشفت الشركة العديد من الثغرات الأمنية المثيرة للاهتمام.

وخلال الفترة ما بين نوفمبر 2020 ويناير 2021، تم تصنيف أغلبية الهجمات على الشبكات على أنها خطرة (75%).

CVE-2020-29227 وCVE-2020-17519 وCVE-2020-28188 وقد ظهرت العديد من الثغرات الأمنية من نوع التي تم استغلالها على نحو مستمر اعتباراً من أواخر عام 2020 إلى أوائل عام 2021.

ومن خلال الاستفادة من جدران الحماية من الجيل التالي من بالو ألتو نتوركس واستخدامها كمستشعرات متكاملة، تمكّن الباحثون في الشركة من عزل الأنشطة الضارة عن حركة البيانات الآمنة في الفترة ما بين نوفمبر 2020 وحتى يناير 2021، ومن ثم معالجة حركة البيانات الضارة بناء على مقاييس عدة مثل عناوين بروتوكولات الإنترنت والمنافذ وأوقات تسجيل الأحداث.

وهذا ما ساعد على تحديد كل هجوم على حدة بطابع خاص به، وبالتالي التخلص من أية بيانات خاطئة محتملة. كما قام الباحثون بعد ذلك بربط البيانات المتكررة بسمات أخرى، مثل فئات الهجوم والتحليلات الخاصة بشركات

التصنيع، بغية الاستدلال على توجهات الهجمات المحتملة مع مرور الوقت، والحصول على صورة كاملة لطبيعة مثل هذه التهديدات.

ومن بين 6.09 مليون من الحالات التي تم تسجيلها ضمن حركة البيانات، فإن ما مجموعه 3.47 مليون حالة هي كانت الأكثر استغلالاً من قبل المهاجمين، وذلك على CVEs هجمات حقيقية، وقد تبين أن الثغرات الأمنية من نوع الأرجح بسبب أعداد العملاء الكبيرة المرتبطة بعمليات استخدام واسعة للبرمجيات والأجهزة المختلفة.

أما عن منشأ الهجمات على الشبكات، فقد تبين أن روسيا هي المصدر الأول لهذه الهجمات، تليها الولايات المتحدة والصين. ومع ذلك، فإننا ندرك أن المهاجمين يمكن أن يكونوا قد استفادوا من الخوادم الوكيلة والشبكات الخاصة .في تلك البلدان، بغية إخفاء مواقعهم الحقيقية VPNs الافتراضية