هجمات طلب الفدية ضد Kaseya تهدد الشركات العالمية

الأحد 4 يوليو 2021 07:48 م

بدأ المتسللون هجومًا عالميًا باستخدام برامج طلب الفدية، حيث أصابوا أكثر من 1000 شركة، وأجبر ذلك سلسلة متاجر البقالة Coop في السويد على إغلاق مئات المتاجر.

وفيما يبدو أنه أحد أكبر هجمات سلسلة التوريد حتى الآن، اخترق المتسللون Kaseya، مورد برامج إدارة تكنولوجيا المعلومات، من أجل نشر برامج طلب الفدية لمقدمي الخدمات المدارة الذين يستخدمون تقنيتها، وكذلك لعملائهم.

وقالت مجموعة Huntress Labs للأمن السيبراني إنها حددت 20 من مزودي الخدمة المُدارين المخترقين، حيث وقع أكثر من 1000 من عملائها ضحية لهجمات برامج طلب الفدية.

من بين الضحايا، قالت شركة Coop في السويد إنها أغلقت جميع متاجرها البالغ عددها 800 باستثناء خمسة بعد أن أدى الهجوم إلى توقف نظام التسجيل وخروج الخدمة الذاتية عن العمل.

وقالت الشركة إن Coop تأثرت بعد إصابة مزود الخدمة المدارة Vissma Escom.

وعزت مجموعة Huntress Labs الهجمات إلى مجموعة REvil المرتبطة بروسيا، التي ادعى مكتب التحقيقات الفيدرالي أنها وراء الهجوم الأحدث ضد مورد لحوم البقر JBS.

وقال الرئيس الأمريكي جو بايدن إنه أمر الوكالات الحكومية الأمريكية بالتحقيق في من يقف وراءها. وأضاف: كان التفكير الأولي أنه لم تكن الحكومة الروسية، ولكننا لسنا متأكدين بعد.

وتمثل هذه الحادثة المثال الأحدث على اختراق المتسللين لسلسلة توريد تكنولوجيا المعلومات من أجل مهاجمة الضحايا على نطاق واسع، من خلال اختراق مزود واحد فقط.

وظهر في العام الماضي أن متسللين روسيين مدعومين من الدولة قد اخترقوا مجموعة برمجيات SolarWinds لتكنولوجيا المعلومات. وذلك من أجل اختراق شبكات البريد الإلكتروني للوكالات والشركات الفيدرالية الأمريكية.

وقالت شركة Kaseya إنها كانت ضحية هجوم إلكتروني معقد وإن نحو 40 من عملاءها المباشرين البالغ عددهم 36000 قد تأثروا.

هجمات طلب الفدية تهدد الشركات العالمية
حثت Kaseya أولئك الذين يستخدمون أداة خادم VSA المخترقة، التي توفر المراقبة عن بعد، على إيقاف تشغيلها.

وأضافت الشركة: نعتقد أننا حددنا مصدر الثغرة الأمنية ونعمل على تطوير تصحيح للتخفيف من المشكلة لعملائنا المحليين.

وقال مكتب التحقيقات الفيدرالي إنه يحقق في هجمات برنامج طلب الفدية. وكان المكتب يعمل مع Kaseya ووكالة الأمن السيبراني وأمن البنية التحتية الأمريكية للاتصال بالضحايا.

وتعد هذه الحملة الأحدث في سلسلة من هجمات برامج طلب الفدية هذا العام. بما في ذلك هجوم على خط الأنابيب Colonial في أمريكا، الذي دفع إدارة بايدن إلى تعهدات بقمع الجناة.

وفي قمة جنيف الشهر الماضي، حث الرئيس جو بايدن الرئيس الروسي فلاديمير بوتين على كبح جماح قراصنة برامج طلب الفدية