تقرير خطير يكشف عن هيمنة غير مسبوقة لبرمجيات الفدية على الإنترنت ونصائح لحماية بياناتك

فى اليوم العالمي لمكافحة برمجيات الفدية في ١٢ مايو، كشفت أحدث أبحاث كاسبرسكي عن اتجاه مثير للقلق في مشهد الأمن السيبراني العالمي، حيث مثلت هجمات برمجيات الفدية ثلث الحوادث السيبرانية في عام ٢٠٢٣.

ويسلط التقرير الضوء على التهديد المتصاعد لمجموعات برمجيات الفدية الموجهة والتي شهدت زيادة بنسبة ٣٠٪ على مستوى العالم مقارنة بعام ٢٠٢٢، بجانب زيادة عدد الضحايا المعروفين بنسبة ٧١٪.

كشفت أبحاث شركة كاسبرسكي، التي غطت عامي ٢٠٢٢ و٢٠٢٣، عن تصعيد مقلق من مجموعات برمجيات الفدية المُستهدفة.

وأشارت البيانات إلى زيادة عالمية مذهلة في عدد هذه المجموعات، حيث ارتفعت بنسبة ٣٠٪ مقارنة بعام ٢٠٢٢، وصاحب ذلك زيادة قدرها ٧١٪ في عدد الضحايا المعروفين لهجماتها. على عكس الاعتداءات العشوائية، توجه هذه المجموعات الموجهة أنظارها نحو الوكالات الحكومية، والمنظمات البارزة، وأفراد مُحددين داخل المؤسسات. ومع استمرار المجرمين السيبرانيين في تنظيم هجمات معقدة وواسعة النطاق، أصبح تهديدهم للأمن السيبراني أكبر من أي وقت مضى.

في عام ٢٠٢٣، برزت برمجية Lockbit ٣,٠ باعتبارها أكثر برمجيات الفدية انتشاراً، حيث استفادت من تسريب برمجية بناء في عام ٢٠٢٢ لتنتج العديد من الإصدارات المخصصة والموجهة إلى منظمات حول العالم. واحتلت برمجية BlackCat/AlphV المرتبة الثانية، حتى ديسمبر ٢٠٢٣، عندما أدت الجهود التعاونية لمكتب التحقيقات الفيدرالي (FBI) والوكالات الأخرى لتعطيل عملياتها. ومع

ذلك، سرعان ما عادت برمجية BlackCat، مما يؤكد مرونة مجموعات برمجيات الفدية. وفي المرتبة الثالثة، جاءت برمجية CL0p، حيث اخترقت نظام نقل الملفات المُدار MoveIt، مما أثر على أكثر من ٢,٥٠٠ منظمة بحلول ديسمبر ٢٠٢٣، وفقًا لشركة الأمن النيوزيلندية Emsisoft.

وفي تقرير «حالة برمجيات الفدية ٢٠٢٣»، حددت كاسبرسكي العديد من عائلات برمجيات الفدية الجديرة بالملاحظة، بما يشمل BlackHunt، وRhysida، وAkira، و Mallox، و3AM. علاوة على ذلك، ومع تطور مشهد برمجيات الفدية، تظهر مجموعات أصغر وأصعب، مما يشكل تحديات جديدة تواجه سلطات إنفاذ القانون.

ووفقًا للأبحاث، أدى ظهور منصات برمجيات الفدية كخدمة (RaaS) إلى زيادة تعقيد مشهد الأمن السيبراني، مما يؤكد الحاجة لاتخاذ تدابير استباقية.

لاحظ فريق الاستجابة للحوادث في شركة كاسبرسكي أن حوادث برمجيات الفدية كانت مسؤولة عن ثلث حوادث الأمن السيبراني في عام ٢٠٢٣. وفي البحث، برزت الهجمات عبر المقاولين ومزودي الخدمات كمحاور أساسية، مما سهل تنفيذ الهجمات واسعة النطاق بفعالية مثيرة للقلق. بشكل عام، أظهرت مجموعات برمجيات الفدية فهماً متقدماً لنقاط الضعف في الشبكة، حيث استخدمت مجموعة متنوعة من الأدوات والأساليب لتحقيق أهدافها. كما استخدمت المجموعات أدوات أمنية معروفة، واستغلت الثغرات الأمنية المتاحة للعامة والأوامر الخاصة بنظام التشغيل Windows للتسلل إلى ضحاياها، وهو ما يسلط الضوء على الحاجة لتدابير أمن سيبراني قوية للتصدي لهجمات برمجيات الفدية وعمليات سرقة المواقع.

علق ديمتري جالوف، رئيس مركز أبحاث فريق البحث والتحليل العالمي (GReAT) بشركة كاسبرسكي: «مع انتشار برمجيات الفدية كخدمة وتنفيذ المجرمين السيبرانيين لهجمات معقدة بشكل متزايد، يصبح التهديد للأمن السيبراني أكثر حدة. وما تزال هجمات برمجيات الفدية تشكل تهديداً هائلاً، حيث تتسلل إلى القطاعات الحيوية وتخترق الشركات الصغيرة دون تمييز بينها. ولمكافحة هذا التهديد المتفشي، من الضروري للأفراد والمؤسسات.

وقدمت كاسبرسكيعدة نصائح للمؤسسات لحماية عملياتها من هجمات برمجيات الفدية:

١. احرص دائماً على تحديث البرمجيات على جميع أجهزتك لمنع المهاجمين من استغلال الثغرات الأمنية والتسلل لشبكتك.

٢. ركز استراتيجيتك الدفاعية على اكتشاف الحركة الجانبية ضمنها وتسريب البيانات عبر الإنترنت. انتبه بشكل خاص لتدفق البيانات الصادرة لاكتشاف اتصالات المجرمين السيبرانيين بشبكتك.

٣. قم بإعداد نسخ احتياطية غير متصلة بالإنترنت من بياناتك، بحيث لا يتمكن المتطفلون من العبث بها، وتأكد من أنه يمكنك الوصول إليها بسرعة عند الحاجة أو في حالات الطوارئ.

٤. قم بتمكين حلول الحماية من برمجيات الفدية على جميع النقاط الطرفية. فعلى سبيل المثال، هناك أداة حماية مجانية للحواسيب والخوادم من برمجيات الفدية والبرمجيات الخبيثة الأخرى.

٥. قم بتثبيت حلول مضادة للتهديدات المستعصية المتقدمة (anti-APT) وحلول الاكتشاف والاستجابة للنقاط الطرفية (EDR)، مما يتيح قدرات اكتشاف وتحديد التهديدات المتقدمة، والتحقيق فيها، وتصحيح الحوادث في الوقت المناسب.

٦. قم بتزويد فريق مركز العمليات الأمني (SOC) الخاص بك بإمكانية الوصول إلى أحدث معلومات التهديدات وتطوير مهاراتهم بانتظام من خلال التدريب الاحترافي.