الخليج

اقتصاد, تقنية وسيارات

11 أغسطس 2023 21:17 مساء

قرصنة الحسابات السحابية لكبار المسؤولين في 100 منظمة عالمية

«دبي: «الخليج

كشفت دراسة بحثية صادرة عن «بروف بوينت» عن أن ما لا يقل عن 35% من هجمات الاستيلاء على الحسابات خلال في ظل مواصلة قراصنة الإنترنت تطوير(MFA) العام الماضي كانت مزودة بنظام المصادقة متعددة العوامل أساليبها للاستيلاء على الحسابات، بهدف سرقة البيانات، ونقل البرامج الضارة، أو استخدام صلاحيات الوصول إلى يعتبر تطوراً عن مصادقة كلمة المرور فقط، وقد زاد استخدامه خلال MFA الحساب لأغراض خبيثة. على الرغم من أن السنوات القليلة الماضية في المؤسسات، إلا أنه لم يمنع من وقوع انتهاكات أمنية.

وفقاً للتقرير؛ يستخدم قراصنة الإنترنت الآن أتمتة متقدمة جديدة لتحديد الوقت الفعلي بدقة ما إذا كان المستخدم المتعرض للتصيّد عبر الإنترنت هو ملف عالي المستوى حيث يركزون على الفور على الاستيلاء على تلك الحسابات، متجاهلين في الوقت نفسه الملفات الأقل مكسباً التي تعرضت للتصيّد.

مما يمكن من الوصول إلى أطقم (PhaaS) «قام قراصنة الإنترنت بإنشاء «التصيّد مع التوثيق متعدد العوامل كخدمة مُعدة مسبقاً للخدمات عبر الإنترنت مثل جي ميل ومايكروسوفت ودروب بوكس وفيسبوك وتويتر. يمكن للقراصنة بسهولة إطلاق حملات باستخدام واجهة نقر واحد تتيح خيارات قابلة للتخصيص، مثل اكتشاف الروبوتات واكتشاف الوكلاء وتحديد الجغرافيا. هذه الواجهة النسبياً بسيطة ومنخفضة التكلفة أدت إلى زيادة كبيرة في عمليات التصيّد مع التوثيق متعدد العوامل.

حزمة تصيّد

وتشكل «إيفل بروكسي»، خطورتها كونها تمثل حزمة تصيّد شاملة سهلة الحصول عليها وتكوينها وإعدادها؛ حيث سلط التقرير الضوء على تحديد فجوة مقلقة في الوعي العام بخطورة وأضرار محتملة ل «إيفل بروكسي».

منذ أوائل شهر مارس، راقب باحثو «بروف بوينت» حملة مشتركة مستمرة باستخدام «إيفل بروكسي» لاستهداف آلاف حسابات مستخدمي مايكروسوفت 365. تم إرسال حوالي 120,000 رسالة احتيالية إلى مئات المؤسسات المستهدفة في جميع أنحاء العالم بين مارس ويونيو 2023.

استهدف المستخدمون المستهدفون العديد من الأهداف ذات القيمة العالية، مثل المديرين التنفيذيين ونواب الرؤساء في الشركات الرائدة، والذين تقدرهم بشكل خاص جهات التهديد بسبب قدرتهم المحتملة على الوصول إلى البيانات الحساسة والأصول المالية. من بين المئات من المستخدمين الذين تعرضوا للاختراق. حيث أشار التقرير إلى 39٪ منهم من فئة المديرين التنفيذيين منهم 17٪ منهم رؤساء المالية، و9٪ منهم رؤساء ومديرون تنفيذيون. أظهر قراصنة أيضاً اهتماماً بالإدارة على مستوى أدنى، حيث ركزوا جهودهم على الموظفين الذين يمتلكون وصولاً إلى الأصول المالية أو المعلومات الحساسة.

الوكيل المعكوس

تُعد تهديدات الخادم الوكيل المعكوس مثل «إيفل بروكسي» تهديداً قوياً في منظومة التهديدات المتطورة الحالية، حيث تتجاوز أدوات التصيّد القديمة والأقل قدرة. لقد ارتفعت شهرتها بشكل كبير وكشفت عن ثغرات حاسمة في استراتيجيات الدفاع لدى المؤسسات. ولهذا السبب، يقوم قراصنة الإنترنت بالتحول بسرعة إلى أدوات التصيّد المتقدمة سهلة الاستخدام، مما يؤدي إلى زيادة فاعلية وسرعة الهجمات المتداخلة. على الرغم من أن هذه الهجمات تبدأ من خلال البريد الإلكتروني، إلا أن هدفها النهائي هو اختراق واستغلال حسابات مستخدمي السحابة القيمة والأصول والبيانات. وهذا المخاوف تتكرر في دولة الإمارات العربية المتحدة، حيث تتصدر جرائم البريد الإلكتروني قائمة أكبر التهديدات وفقاً لتقرير: وجهات نظر رؤساء أمن المعلومات للعام 2023 الصادر عن «بروف بوينت».

يستخدم قراصنة الإنترنت تقنيات متعددة، بما في ذلك الحركة الجانبية وانتشار البرمجيات الضارة؛ حيث يقومون بدراسة ثقافة المؤسسات المستهدفة وهياكلها التنظيمية وعملياتها، لتجهيز هجماتهم وزيادة نسب النجاح. قام وبيع (HaaS) المهاجمون بتنفيذ جرائم مالية وتنفيذ عمليات سحب البيانات أو تنفيذ عمليات الاختراق كخدمة الوصول إلى حسابات المستخدمين المخترقة.