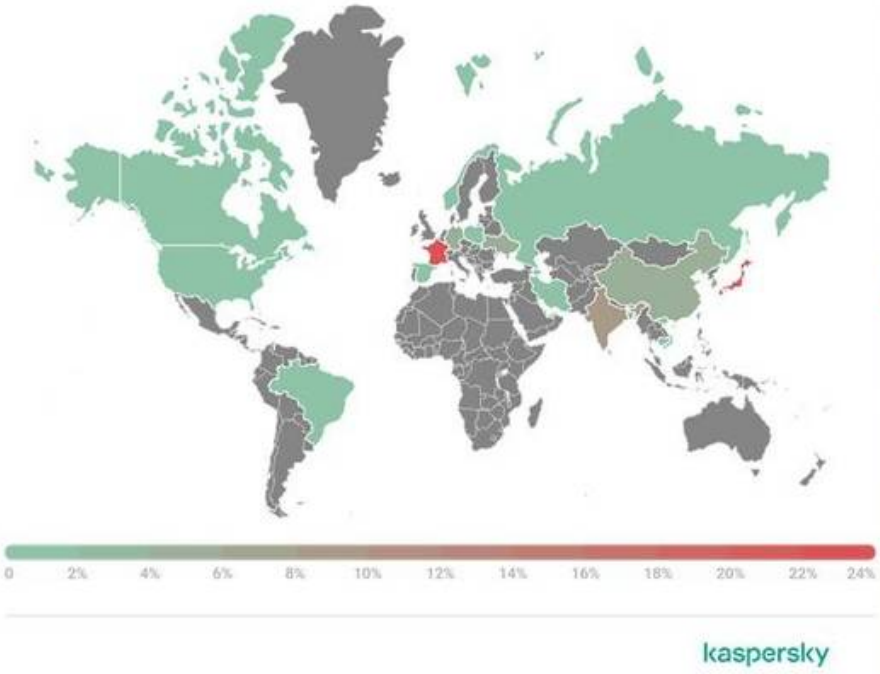
الخليج

اقتصاد, تقنية وسيارات

9 فبراير 2022 19:57 مساء

اكتشاف حملة رقمية خبيثة.. وخمس دول الأكثر تضراراً



«دبي: «الخليج

وكانت تستهدف مناطق Roaming Mantis اكتشفت كاسبرسكي أن حملة تخريبية رقمية خبيثة أُطلق عليها اسم آسيوية في الأغلب، قد بدأت تنتقل لتصيب أهدافاً في الدول الغربية. ووجد خبراء كاسبرسكي أن الحملة التي تعمل على توسعة نطاق الإصابات عبر الرسائل النصية القصيرة التصيدية التي توجّه المستخدمين إلى محتوى خبيث، بدأت تضرب أهدافاً جديدة في ألمانيا وفرنسا. وتنشر الجهة التخريبية التي تقف وراء الحملة برمجية خبيثة خاصة بالهواتف المحمولة وصفحات تصيّد لجمع المعلومات الخاصة بالمستهدفين من أجل سرقة أموالهم. ويرسل الجهاز المصاب إلى المجموعة التالية من الأهداف، كتلك الموجودة في SMiShing بعد ذلك الرسائل النصية التصيدية، التي تُسمّى قائمة جهات الاتصال.

التي استهدفت Roaming Mantis وكان باحثو كاسبرسكي اكتشفوا في إبريل/ نيسان 2018 لأول مرة البرمجية فقط، وركّزت نشاطها في مناطق آسيا، وبالتحديد كوريا الجنوبية Android آنذاك الهواتف الذكية العاملة بنظام

وبنجلاديش واليابان. وسرعان ما تطوّرت الحملة بعد ذلك، فمنذ عام 2018، استخدمت العصابة أساليب هجوم مختلفة كما وسّعت حضورها DNS مثل رسائل التصيد البريدية والتعدين ورسائل النصية القصيرة التصيدية واختراق الجغرافي بإضافة دول أوروبية إلى مناطقها المستهدفة.

الأكثر تضرُّراً

الدول الأكثر تضرراً من الحملة هي فرنسا واليابان والهند وألمانيا وكوريا الجنوبية.

لصفحة مقصودة. فإذا نقر URL وعادةً ما تحتوي الرسائل النصية القصيرة التصيدية على وصف قصير جداً وعنوان في السيناريو .Roaming Mantis المستخدم على الرابط وفتح الصفحة يحدث أحد سيناريوهين متبعين في حملة الإلكتروني الرسمي Apple يجري توجيهه إلى صفحة تصيّد تحاكي موقع iOS الأول، إذا كان يستخدم نظام التشغيل ببرمجية خبيثة Android ويُطلب منه إدخال بيانات الاعتماد. أما في السيناريو الثاني، فيصاب جهاز.

إلى أهداف جديدة عبر الجهاز المصاب؛ وذلك من قائمة جهات SMiShing وتبدأ العصابة في إرسال مزيد من رسائل اتصال المستخدم وأرقام هواتف يجري إنشاؤها. ولا يُبدي متلقي الرسائل النصية حرصاً كبيراً على اتّقاء التهديدات، باعتبارها قناة اتصال تتسم بالطابع الشخصي؛ إذ لا يتوقع المستخدمون عادةً تلقي رسائل خبيثة من أشخاص يعرفونهم.

في فرنسا وألمانيا بالنشاط إلى درجة أن الشرطة ووسائل Androidو iOS هذا، وقد اتسمت هذه الحملة ضد مستخدمي الإعلام المحلية نشرت تنبيهات بشأن رسائل التصيد SMiShing.

على مواقع ألمانية وفرنسية SMiShing تنبيهات تُحذّر من رسائل

المصاب، Android وأعدّت العصابة ميزة في البرمجية تمكّنها من التحقق دائماً من المنطقة التي يوجد بها جهاز لعرض الرسالة باللغة المناسبة. وقد استخدمت هذه الميزة في الإصدارات السابقة من الحملة للتحقق من ثلاث مناطق: هونج كونج وتايوان واليابان. ولاحظ خبراء كاسبرسكي تحديثاً في الإصدار الأخير يتضمّن إضافة ألمانيا وفرنسا إلى قائمة المناطق الجديدة التي يجري التحقق منها. ويتيح استخدام اللغة الأصلية للمناطق المستهدفة المجال أمام العصابة للتلاعب في تفكير المستخدم وإقناعه بمشاركة معلوماته الشخصية وتفاصيله المصرفية.

وثمّة تعديل جديد حدث في الأوامر الواردة عبر المنفذ الخلفي، مقارنة بالإصدارات السابقة؛ إذ أضاف المطور أوامر لسرقة الصور من الأجهزة المصابة، إلا أنه لم يُعثر على معلومات حول طرق استخدام الصور المسروقة، إلا أن مجرمي الإنترنت في الأغلب يستخدمون الصور الشخصية للحصول على المال من خلال ابتزاز ضحاياهم.

وأكّد سوغورو إيشيمارو الباحث الأمني الأول في فريق البحث والتحليل العالمي التابع لكاسبرسكي، أن حملة Roaming Mantis تطوّرت كثيراً على مدى السنوات الخمس الماضية، مشيراً إلى أنها ابتكرت طرقاً جديدة للهجوم، وحرصت على التوسّع في البلدان المستهدفة. وتوقع الخبير الأمني أن تستمر هذه الهجمات في عام 2022 بدافع من الرغبة القوية في الحصول على المال، خاصة مع ظهور مزايا المنفذ الخلفي الجديدة التي تسمح للعصابة التي تقف وراءها بالحصول على صور الضحايا. ونحن نبحث باستمرار عن أحدث أنشطة هذه الحملة ونقوم بالإبلاغ عنها، حرصاً منا على أمن المستخدمين في أنحاء العالم.

ماذا تفعل؟

Roaming Mantis: وتوصي كاسبرسكي المستخدمين باتباع التدابير التالية لحماية أنفسهم من هجمات

- حتى إذا بدت الرسالة غير مريبة، يجب التحقّق من SMS المشبوهة المرسلة في رسائل URL لا تنقر على عناوين قبل الوصول إليها URL اسم نطاق عنوان.

- حتى إذا وصلت رسالة نصية أو بريد إلكتروني من أحد الأشخاص المقربين، فتذكّر أنه من الممكن أيضاً أن تكون حساباتهم تعرضت للاختراق، فكن حذراً دائماً، وتعامل مع الروابط والمرفقات باهتمام حتى إذا بدت الرسالة ودية.

- الرسائل الواردة من الجهات الرسمية، كالبنوك ووكالات الضريبة ومتاجر التسوق الرقمية ووكالات السفر وشركات الطيران وما إلى ذلك، تتطلب أيضاً التدقيق؛ بل وحتى الرسائل الداخلية الواردة من شركتك، فليس من الصعب اختلاق رسالة مزيفة تبدو حقيقية.

- تجنّب تثبيت تطبيقات من مصادر غير موثوق بها.

- احرص على تثبيت حلّ أمني موثوق به واتبع توصياته. ستحلّ الحلول الآمنة أغلب المشكلات تلقائياً وتنبهك إذا لزم الأمر.