

إحباط 500 مليون هجمة تصيد حول العالم



- خدمات التوصيل «المجال الأكثر استهدافاً»
- غالبية المحاولات عن طريق «واتساب» و«تلغرام» و«فايبر»
- تحديثات مزيفة وميزة توثيق الحساب على «منصات التواصل»

«دبي»: الخليج

أوقف نظام كاسبرسكي لمكافحة التصيد أكثر من 500 مليون محاولة للوصول إلى مواقع ويب احتيالية على مستوى العالم في 2022. ويزيد هذا الرقم بمرتين مقارنة بأرقام 2021. وتأثر 7.2% من الأفراد والمؤسسات بهجمات التصيد في منطقة الشرق الأوسط؛ إذ اكتشفت الهجمات على أجهزتهم وتم إيقافها

وتعتمد هجمات البريد غير المرغوب فيه وهجمات التصيد على أساليب الهندسة الاجتماعية المعقدة، ما يجعلها شديدة الخطورة لغير العارفين بها، وذلك بالرغم من أن تلك الهجمات ليست بالضرورة معقدة تقنياً. ويتمتع المحتالون بمهارة

إنشاء صفحات ويب تصيّد مماثلة لمواقع الويب الأصلية، لتجمع بيانات المستخدمين الخاصة أو تدفعهم إلى تحويل الأموال إلى المحتالين الذين يستهدفون الأفراد والمؤسسات.

واكتشف خبراء كاسبرسكي ارتفاعاً في تحوّل مجرمي الإنترنت خلال عام 2022 إلى هجمات التصيّد. ونجح نظام كاسبرسكي لمكافحة التصيّد في منع 507,851,735 محاولة للوصول إلى محتوى احتيالي في عام 2022، وذلك على مستوى العالم، ويزيد هذا الرقم بمقدار الضعفين على عدد الهجمات التي تم إحباطها في عام 2021.

وكانت «خدمات التوصيل» المجال الأكثر استهدافاً بهجمات التصيّد العام الماضي، إذ يرسل المحتالون رسائل بريد إلكتروني مزيفة تبدو كأنها واردة من شركات توصيل معروفة وتدعي بأن هناك مشكلة في التسليم، بحيث تتضمن رابطاً إلى موقع ويب مزيف يطلب معلومات شخصية أو تفاصيل مالية. وقد تنكشف هوية المستخدم ومعلوماته المصرفية إذا وقع ضحية لعملية الاحتيال هذه، فيفقد أموالاً أو تُباع معلوماته على الويب المظلمة.

وسلّط خبراء كاسبرسكي الضوء أيضاً على توجّه عالمي برز في مشهد التصيّد خلال العام 2022، تمثل في زيادة توزيع الهجمات من خلال تطبيقات التراسل، فجاءت غالبية المحاولات المحظورة من واتساب وتلغرام ثم فايبير.

كذلك برز طلب متزايد بين مجرمي الإنترنت على بيانات اعتماد دخول المستخدمين إلى حسابات وسائل التواصل الاجتماعي، حيث يستغلون فضول الأفراد نحو الجديد ورغبتهم في الخصوصية ويقدمون تحديثات مزيفة ويعرضون، زيفاً، ميزة توثيق الحساب على منصات وسائل التواصل الاجتماعي.

مثال في وسائل التواصل الاجتماعي

ووجد الخبراء أيضاً أن عمليات الاحتيال المتعلقة بالعملات الرقمية والجائحة ما زالت تُستخدم من قبل المهاجمين في محاولات التصيّد بهدف سرقة معلومات حساسة من الأشخاص الذين يتسمون بالخوف والقلق من الظروف المحيطة، مستغلين مخاوفهم.

وأكدت أولغا سفيستونوفا خبيرة الأمن الرقمي أن التصيّد أحد أكثر التهديدات انتشاراً وتخريباً في مجال الأمن الرقمي، مشيرة إلى كونها بوابة للعديد من أسوأ التهديدات الرقمية، وقالت: «تمثل صفحات التصيّد الخطوة الأولى في سلسلة طويلة من الحوادث التي يمكن أن تؤدي إلى سرقة الهوية وخسارة المال والإضرار بالسمعة لكل من الأفراد والمؤسسات، لذلك ندعو الجميع إلى فهم أبعاد التهديدات وعواقبها واتخاذ الإجراءات اللازمة لحماية أنفسهم».