الخليج

أخبار الدار, حوادث وقضايا

9 أكتوبر 2023 00:33 صباحا

زيادة ربع سنوية في هجمات التصيد الاحتيالي عبر الإنترنت بالإمارات

دبي: محمد إبراهيم

كشف رينزي جونغمان، خبير الأمن السيبراني والتهديدات في منطقة الشرق الأوسط وشمال إفريقيا، والمستشار بمؤسسة «مانديانت»، أن هناك زيادة ربع سنوية في هجمات التصيد الاحتيالي وعمليات الاحتيال عبر الإنترنت في مختلف المجتمعات بما فيها الإمارات، وفقاً لدراسات وتقارير دولية مختلفة.

في وقت حذرت «دبي الرقمية» من عمليات اختراق الهواتف عبر تطبيق «واتس آب»، إذ زادت في الساعات الأخيرة محاولات اختراق الهواتف، حيث يلجأ المحتالون إلى إرسال رسائل عبر تطبيق «واتس آب» من أسماء أشخاص يعرفهم المتلقي، ويُطلب منه الضغط على رابط لدخول مجموعة ما، ويتم من خلاله محاولة الاستيلاء على البيانات عبر «واتس آب» الخاص بالمستخدم.

أسباب 4

ورصد رينزي جونغمان ل«الخليج» في مداخلة هاتفية، 4 أسباب وراء هذه الزيادة، أبرزها ضعف حواجز الحماية القائمة في وجه اختراق المعلومات، ما يسهل على مجرمي الإنترنت القيام بحملات احتيال عبر فضائها الواسع، للأسف، تتوفر البنية التحتية والأدوات والهويات المسروقة وحتى إمكانية الوصول للضحايا التي تم اختراقها مسبقاً للبيع على المنتديات أونلاين، كما توجد حالياً شبكات الجرائم الإلكترونية «كخدمة»، وتعمل باحترافية وعلى نطاق واسع، ما يعزز من إمكانيات الاختراق والوصول إلى المعلومات.

وأشار إلى السبب الثاني الذي يكمن فيما يعرف ب«الإفلات من العقاب»، لقدرة المهاجمين على إخفاء هوياتهم والبقاء شبه مجهولين عبر الإنترنت، فضلاً عن حجم المشكلة وطبيعة الجرائم السيبرانية العابرة للحدود، حيث تكون الضحية والبنية التحتية والجاني في أماكن جغرافية مختلفة ومتعددة، ولا يوجد اتصال مباشر بينهم، ما يجعل من الصعب التحقيق في الجريمة ومقاضاتها، كما يعمل مجرمو الإنترنت بثقة لمعرفتهم أن احتمالية مواجهته لعواقب أفعالهم شبه معدومة.

زيادة الهجمات

وأكد أن بعد الضحايا عن المجرمين يعد سبباً جديداً في زيادة الهجمات وتفاقمها، إذ أن مجرمي الشوارع يواجهون ضحاياهم عند سرقة ممتلكاتهم، على عكس مجرمي الإنترنت وضحاياهم، فكلاهما مجهولان يرى كلاهما الآخر، وهنا حاجز بينهما في مشهد الجرائم الإلكترونية، ما أذاب الشعور بالذنب وألم الضمير لدى أصحاب هذه النوعية من الجرائم لأنه لا يشعر بالتأثير النفسي والمالي للضحايا من جراء أفعالهم.

وأكد أن الجريمة الالكترونية مثلها كأي جريمة أخرى، تتكرر هجمات التصيد الاحتيالي والقرصنة والاحتيال وتزداد نسبتها متى حققت هذه العمليات أي نجاح، وهنا تأتي أهمية أن يراقب الأشخاص الشركات والمؤسسات وترصد بفعالية التهديدات الرقمية المماثلة، حتى يتمكنوا من اتخاذ الإجراءات اللازمة، على سبيل المثال، إذا اكتشف أحد البنوك قيام أحد المجرمين الإلكترونيين بإنشاء موقع إلكتروني مزيف وتصميمه ليبدو وكأنه موقع البنك الإلكتروني من أجل الاحتيال على عملاء البنك، فيجب التواصل بسرعة مع موفر خدمة استضافة الموقع الإلكتروني، لإزالته أو التعاون مع الجهات القانونية لتحقيق ذلك، من خلال اتخاذ خطوات استباقية لمراقبة مثل هذه التهديدات، ستتمكن الشركات بحماية اسمها وسمعتها وعملائها.

الأكثر شيوعاً

وفي وقفته مع عمليات الاحتيال والأساليب الأكثر شيوعاً لخداع الأفراد، والوصول غير المصرح به إلى معلوماتهم أو أنظمتهم أو عناوينهم، أفاد بأن الأساليب متعددة ومتنوعة وتحتاج إلى الوعي الكافي من المستهدف لمنع هذه الهجمات، فقد يتظاهر المهاجم بأنه يمثل البنك أو الشرطة أو خدمات البريد، ويتظاهر بأنه يتصل نيابة عن شركة معروفة وذات ثقة، أو يقومون بإرسال رسائل نصية متكررة («تم إيقاف بطاقتك! عليك دفع غرامة الآن! تم تأخير طردك البريدي!)، ما يخلق إحساساً بالإلحاح وعدم اليقين لدى الضحايا يدفعهم إلى مشاركة بياناتهم الخاصة.

ووصفت مانديانت في تقرير حديث لها، كيف يستهدف مجرمو الانترنت الأفراد بشكل متزايد بفرص عمل مزيفة، وغالباً ما يتم استهداف الشركات التي تبحث عن مهارات فريدة وذلك بإرسال سيرة ذاتية مزيفة لها. بمجرد أن يفتح مسؤول التوظيف الملف، يتم تثبيت البرامج الضارة على نظام الشركة.

أهداف قيمة

وأضاف أن استهداف شركات أو صناعات معينة يمكن مجرمي الإنترنت من الوصول إلى أهداف قيمة، ويسمح لجهات التجسس بجمع معلومات في غاية السرية حول مواضيع محددة للغاية، ومن المؤكد أن المؤسسات التي تتمتع بجاهزية الحماية تستخدم معلومات قيمة حول التهديدات ووسائل حديثة لاكتشاف الهجمات والتصدي لها بسرعة فوراً عند حدوثها، فقوة هذه الشركات تكمن في معرفتها بالجهات التي تخطط لمهاجمتها، ما يسمح لها باتخاذ إجراءات وقائية فاعلة.

وفي شرحه لمفهوم الهندسة الاجتماعية أو القرصنة البشرية وكيفية استخدامها في عمليات الاحتيال، أفاد خبير الأمن السيبراني والتهديدات في منطقة الشرق الأوسط وشمال إفريقيا بأن الهندسة الاجتماعية تعد نوعاً من الهجمات الإلكترونية التي تعتمد على التفاعل البشري لخداع الضحايا وإقناعهم بإفشاء معلومات حساسة أو اتخاذ إجراءات تهدد أمنهم، إذ يستخدم المهاجمون مجموعة متنوعة من الأساليب للتلاعب بالضحايا، بما في ذلك التصيد الاحتيالي، والتصيد الاجتماعي أو الانتحالي، شيء مقابل شيء، وهذا النوع من هجمات الهندسة الاجتماعية يقدّم فيها المهاجم للضحية شيئاً ما مقابل معلوماته الشخصية.

مصدر رسمي

وأكد أن هجمات الهندسة الاجتماعية فعالة للغاية لأنها تستغل الطبيعة البشرية، وغالباً ما يكون الناس أكثر استعداداً للثقة بشخص يعرفونه أو شخص يبدو أنه يمثل مصدراً رسمياً موثوقاً به، كما يلجأ المهاجمون للهندسة الاجتماعية لاستغلال مخاوف الناس أو مشاعرهم.

وحول الوعي الكافي بين سكان المنطقة بهجمات التصيد المالي وعمليات الاحتيال أونلاين، أكد أن الوعي موجود ولكن ينقصه التخطيط والتعامل بمسؤولية والتدريب المستمر لفهم ماهية الهجمات الإلكترونية من خلال برامج وحملات وطنية في الإمارات لمعالجة هذا الأمر، مع تصميم وتقديم أنشطة وبرامج تسهم في زيادة الوعي المجتمعي ودعم وتشجيع الشباب على استكشاف مهن في مجال الأمن السيبراني.