

المخططات الثلاثة الأكثر شيوعاً لاختراق البريد الإلكتروني



دبي: «الخليج»

يزداد اهتمام الخبراء بمراقبة الهجمات التي تستهدف اختراق البريد الإلكتروني في الشركات. مثلاً، منعت منتجات كاسبرسكي أكثر من 9,500 هجوم لاختراق البريد الإلكتروني الخاص بالعمل بين مايو ويوليو 2021. وطالت الهجمات شركات في قطاعات النقل الجوي والصناعة والتجزئة وتقنية المعلومات والتوصيل. وتتطلب مثل هذه الهجمات وقتاً وموارد كبيرة، وقد يستمر الإعداد لها من بضعة أسابيع إلى عدة أشهر، فيما قد يؤدي هجوم واحد ناجح إلى إلحاق أضرار بالشركة المستهدفة يمكن أن تصل الخسائر جراه إلى الملايين. وعادةً ما يتخذ المحتالون خطوات تمهيدية لهجماتهم التي تستهدف اختراق البريد الإلكتروني في الشركات، وذلك بالشروع في تبادل رسائل البريد الإلكتروني مع أحد موظفي الشركة لكسب ثقته بالحيلة وتشجيعه على اتخاذ إجراءات تسفر عن إلحاق الضرر بمصالح الشركة أو المعنيين بها من أصحاب المصلحة. وللقيام بذلك، كثيراً ما يلجأ المحتالون إلى حسابات بريد إلكتروني مخترقة للموظفين أو عناوين بريد إلكتروني تشبه في تهجئتها عناوين الشركة الرسمية. كذلك يسرق مجرمو الإنترنت أحياناً بيانات الدخول إلى حساب البريد الإلكتروني لأحد الموظفين سعياً لاستهداف زملائه، لا سيما من أصحاب المناصب العالية. ويسعى المحتالون للحصول على

معلومات سرية عن الشركة، كقاعدة بيانات العملاء أو مستندات الأعمال والمشاريع، وذلك بالرغم من أنهم يهدفون في معظم الحالات إلى سرقة المال من الشركة.

ويسلط خبراء كاسبرسكي الضوء على المخططات أو السيناريوهات الثلاثة الأكثر شيوعاً بين مجرمي الإنترنت لاختراق البريد الإلكتروني في الشركات:
انتحال صفة قيادية

في هذا السيناريو، يتلقى الموظف رسالة بريد إلكتروني مزيفة من زميل أعلى منصباً، في مسعى لإقناع الموظف بمشاركة المعلومات مع «مستشار قانوني» مزعوم، عبر حساب يكون وهمياً، وذلك لسرقة البيانات السرية للشركة. مثال على رسالة بريد إلكتروني مزيفة تدعو لمشاركة البيانات مع «مستشار قانوني» تغيير وهمي في نظام الرواتب.

في هذا السيناريو، يتلقى قسم المحاسبة رسالة من موظف مزعوم يطلب تغيير بياناته المصرفية الخاصة بتحويل راتبه. فإذا قام المحاسب بتغيير التفاصيل المصرفية في نظام كشوف الرواتب، سيذهب راتب الموظف إلى المجرم الذي انتحل شخصية الموظف.

فاتورة مزيفة

ترد هذه الرسالة أيضاً من قسم المحاسبة، ولكنها تبدو في هذا السيناريو وكأنها واردة من مورد أو شركة أخرى، وتتعلق بتأخير مزعوم في سداد قيمة فاتورة ما. فإذا انطلت الحيلة على المحاسب، ستذهب قيمة الفاتورة إلى المجرم المدعي. ويحرص مجرمو الإنترنت دائماً على جمع البيانات بعناية حول ضحاياهم قبل استخدامها لبناء الثقة فيما بينهم سعياً لضمان النجاح في تنفيذ هجمات اختراق البريد الإلكتروني في الشركات، وفقاً لأليكسي مارشنيكو رئيس قسم الأبحاث المتعلقة بأساليب فلترة المحتوى لدى كاسبرسكي، الذي قال إن النجاح يمكن أن يكون حليف المجرمين في شئ بعض هذه الهجمات نظراً لسهولة الحصول على أسماء الموظفين ومناصبهم ومواقع عملهم وتواريخ إجازاتهم وقوائم جهات الاتصال التي يتعاملون معها، وغيرها من البيانات. وأضاف: «يستغل المحتالون عموماً مجموعة واسعة من أساليب الهندسة الاجتماعية لكسب ثقة الضحايا وارتكاب عمليات تخريبية، وهو ما يدفعنا إلى دعوة المستخدمين دائماً إلى توخي الحذر في العمل».

ويوصي خبراء كاسبرسكي الشركات باتباع التدابير التالية لتجنب الوقوع ضحية لهجمات اختراق البريد الإلكتروني: استخدام حلول أمنية موثوق بها تتضمن تقنيات متقدمة لمكافحة التصيد والبريد الإلكتروني غير المرغوب فيه. إثراء المعرفة الرقمية للموظفين عبر منصات تدريبية متخصصة. ويُعدّ تدريب الموظفين على تحديد مبادئ الهندسة الاجتماعية أحد أكثر الطرق فعالية للتصدي لها.

نهي الموظفين عن فتح الرسائل المشبوهة أو الرد عليها، وعن وضع بيانات الشركة السرية على الأنظمة التي تتمتع بإمكانيات الوصول المفتوح وغير المحمي، كالخدمات السحابية. كذلك على الموظفين الامتناع عن مشاركة الكثير من تفاصيل العمل مع مجموعة واسعة من الأشخاص