العرب
الأحد 2019/07/14
السنة 42 العدد 11407

كيف تتجنب تجنيدك كجاسوس على «لينكد إن»

منصة توفر لوكالات الاستخبارات «عملاء» محترفين بشكل أكبر من منصات التواصل الاجتماعي الأخرى

بيئة خصبة لتجنيد العملاء

واشنطن - منذ عام 2016، تفرض السلطات الروسية حظرا على موقع ""لينكد إن"" لرفضه تخزين بيانات المستخدمين الروس وتسليمها للسلطات، في المقابل، تستفيد موسكو من هذا الموقع في عمليات التجسس وجمع المعلومات وتجنيد العملاء من المملكة المتحدة والولايات المتحدة وغيرهما عبر التواصل مع مستخدمي شبكة التواصل المهنية "لينكد إن".

وتستخدم وكالات الاستخبارات دائما معلومات المصادر المفتوحة لتحديد الأشخاص الذين لديهم إمكانية الوصول إلى البرامج أو المعلومات التي يحاولون جمعها. ويزود الإنترنت هذه الوكالات بالمزيد من المعلومات مفتوحة المصدر؛ وبعض المواقع، مثل "لينكد إن"، مفيد بشكل خاص لاكتشاف الأشخاص الذين لديهم إمكانية الوصول إلى المعلومات أو التقنيات المطلوبة.

سكوت ستيورات

المخابرات الصينية تعد من بين أكثر المستخدمين نشاطا في موقع «لينكد إن» والاستفادة منه كأداة للتجنيد

ومؤخرا، أوقفت إدارة الموقع حسابا لروسية حسناء تدعى كيتي جونز، تبين أنه حساب مزيف وهذه الروسية، التي تبين أنها شخصية وهمية وصورتها ليست حقيقية بل من اختراع برنامج ديب فايك، للإيقاع بمشتركين من دوائر المسؤولين الأميركيين والبريطانيين.

ويلفت سكوت ستيوارت، الخبير في التجسس الإلكتروني، في مركز ستراتفور للأبحاث الأمنية والاستراتيجية، إلى أنه من خلال فهم كيفية استخدام وكالات الاستخبارات لهذا الموقع ومنصات وسائل التواصل الاجتماعي الأخرى، فإنه يمكن اتخاذ خطوات لتجنب التهديد أو تخفيفه.

خلايا صينية نشطة

إلى جانب روسيا، تستخدم الصين، نفس الأسلوب على موقع "لينكد إن" لتجنيد عملاء أميركيين ومحاولة الحصول على معلومات وأسرار حكومية وتجارية. وتستهدف الصين الخبراء في مجالات مثل الحوسبة الفائقة والطاقة النووية وتكنولوجيا النانو وأشباه الموصلات وتقنيات التخفي والرعاية الصحية والبذور والطاقة الخضراء.

ويقول مسؤولون أميركيون إن الصين تشكل "التهديد الأكبر" في ما يتعلق بعمليات التجنيد على وسائل التواصل الاجتماعي مثل "لينكد إن". ويشير سكوت ستيوارت إلى أن عدد الحالات المبلغ عنها والمنسوبة إلى الصينيين، بما في ذلك حالات ضباط المخابرات السابقين مثل كيفن مالوري، وهو دبلوماسي أميركي متهم بالتجسس لصالح الصين، وقضايا التجسس للشركات، تشير إلى أن أجهزة المخابرات الصينية هي من بين أكثر المستخدمين نشاطا على موقع "لينكد إن" وتستخدمه كأداة توظيف.

مع ذلك، لا تقتصر هذه الظاهرة على عمليات الاستخبارات الصينية ولا تقتصر حتى على منصات التواصل الاجتماعي الخاصة. ولكن تستخدم جميع وكالات الاستخبارات طرقا مماثلة، كما أوضحت شركة ديلويت، وهي أكبر شركة خدمات مهنية في العالم، بشأن الاختراق المرتبط بإيران الذي حدث واستُخدم فيه "لينكد إن" لكسب ثقة موظف.

وهذا يصعّب من عملية تجنب التهديد، سواء على "لينكد إن" أو على أي منصة أخرى، وفق ستيورات، الذي يرى أن مواجهة التهديد القادم عبر لينكد تتطلب فهما لكيفية استخدام أجهزة الاستخبارات له في عمليات التوظيف. ويمكن تحقيق ذلك من خلال عرض المنصة عبر عدسة دورة توظيف العنصر البشري للاستخبارات.

عملية التوظيف

يشرح سكوت ستيوارت كيف تستخدم وكالات الاستخبارات موقع "لينكد إن"، مشيرا إلى أن عملية التوظيف تتكون من ثلاث مراحل أساسية: الاكتشاف والتطوير والتقاط الهدف. ويمكن تقسيم كل منها إلى خطوات أصغر. ويمكن أن يكون هناك قدر كبير من التباين في العملية حسب الهدف والظروف.

في مرحلة الاكتشاف، يقوم ضباط المخابرات بإدراج الأشخاص الذين لديهم إمكانية الوصول إلى المعلومات المطلوبة على قائمة الأهداف وترتيبهم وفقا لفرص استخراجها.

وقبل ظهور الإنترنت، كان ضباط المخابرات الذين يريدون استهداف شخص ما، في الفريق «أ» على سبيل المثال والتابع لشركة معينة تعمل في مجال التكنولوجيا «ب» أو لديه إمكانية النفاذ إلى البرنامج «ج»، يضطرون إلى القيام ببعض الأعمال الخطيرة. قد تتضمن الخطوات الحصول على قوائم موظفي الشركة أو استخدام بعض الوسائل الأخرى للحصول على أسماء الأشخاص الذين يعملون في مشروع معين في شركة معينة. وفي بعض الحالات، ربما اضطروا إلى تعيين وكيل لهم يستطيع دخول الشركة للمساعدة. وقد يستغرق كل هذا بعض الوقت والجهد، وإذا لم يتم إنجازه بشكل ماهر، فقد يثير الشكوك في الشركة المستهدفة.

ولكن في عالم وسائل التواصل الاجتماعي، يمكن لمسؤولي المخابرات استخدام "لينكد إن" للحصول على قوائم الموظفين في شركة أو وكالة معينة في غضون ثوان. وفي العديد من الحالات، يكتب الموظفون المشاريع أو التقنيات المحددة التي يعملون عليها، حتى أن بعضهم يقدم مستويات الأمان الخاصة بهم.

وعلى الرغم من أن أدوات وسائل التواصل الاجتماعي ليست مضمونة لضباط المخابرات لإنشاء قائمة شاملة للجميع ممن لديهم إمكانية الوصول إلى برنامج أو تقنية، إلا أنه يمكنهم بسهولة بدء هذه العملية. وبالبحث عن زملاء العمل للأشخاص المحددين في البحث الأولي، قد يتمكن ضباط المخابرات من إضافة أشخاص لم يكونوا صريحين في ملفاتهم الشخصية على "لينكد إن" إلى قائمة الأهداف المحتملة.

وبمجرد قيام ضابط المخابرات بتجميع قائمة بالأهداف المحتملة، ستكون الخطوة التالية هي تحديد أفضل احتمالات التوظيف، وما هي الطريقة التي ستعمل بشكل أفضل للفوز بهم. هنا، أيضا، يمكن أن يكون "لينكد إن" مفيدا.

وعلى الرغم من أن الخدمة موجهة نحو المحترفين، ومنظمة بشكل أكبر من منصات التواصل الاجتماعي الأخرى مثل فيسبوك أو إنستغرام، يشارك أعضاؤها عادة معلومات كافية لتقديم أدلة حول طريقة توظيف هذا الشخص.

على سبيل المثال، أولئك الذين يجاملون باستمرار الأشخاص الجذابين قد يكونون مؤهلين لممارسة تنطوي على الإغراء. وبطريقة مماثلة، يمكن أن يكون أولئك الذين يعانون من البطالة هدفا للإغراءات المالية. أو هؤلاء الذين يبدون غير راضين عن وظائفهم، يمكن توظيفهم بدافع الغل والحقد. وأولئك الذين يطلبون الإطراء على الموقع، قد يستجيبون لبعض المديح لشخصياتهم.

تسهل هذه المعلومات الوصول إلى الأهداف المحتملة وإقامة اتصال معها. وإجراء هذه العمليات إلكترونيا يسمح حتى لموظف واحد بتطوير اتصالات مع أهداف متعددة قبل التركيز بشكل أكثر على القلة التي تبدو أكثر تقبلا، وبالتالي زيادة احتمالات النجاح.

ويمكن أن تتطور مرحلة التطوير في عملية التوظيف بشكل مختلف اعتمادا على الهدف النهائي. سيتم تطوير نوع من عمليات التصيد مثل تلك المستخدمة في حالة شركة ديلويت، بشكل مختلف عن العملية التي تتضمن محاولة للقاء وتجنيد المصدر شخصيا. ولكن في كلتا الحالتين، فإن الهدف النهائي لمرحلة التطوير هو إقامة علاقة وبناء درجة من الثقة حتى يمكن الوصول إلى الهدف الاستخباراتي.

وفي ما يتعلق بـ"لينكد إن"، لاحظ سكوت ستيورات العديد من الحالات التي تقوم فيها وكالات الاستخبارات مثل الصين بتطوير علاقة مع هدف من خلال الظهور كمركز أبحاث أو جامعة. وباستخدام هذا المظهر، تدفع الوكالة الهدف إلى كتابة ورقة حول موضوع غير ضار إلى حد ما، ثم تدعوه إلى رحلة مدفوعة التكاليف إلى الصين لعرضه.

وبمجرد وصول "العميل" إلى الصين، سيتم تقييم الأهداف بشكل أكثر تدقيقا، وتتطور العلاقة بشكل أكبر بهدف إنشاء درجة توظيف نهائية. وفي بعض الحالات، ستستخدم وكالة الاستخبارات وثائق (مثل مقاطع الفيديو) للمعاملات السابقة بين ضابط الاستخبارات والهدف كشكل من أشكال الإكراه، إذا لزم الأمر.

التعامل مع التهديد

بمجرد تعيين الهدف رسميا، يمكن الضغط عليه لتوفير معلومات أكثر حساسية. وعلى الرغم من ذكر الصين هنا على وجه التحديد، إلا أن جميع وكالات الاستخبارات تستخدم نفس دورة التوظيف الأساسية هذه، كما تفعل الجهات الفاعلة في مجال المخابرات.

يقول ستيوارت إن هناك طريقتان أساسيتان للتعامل مع التهديد. إحداهما هي تجنب المخاطر والأخرى هي تخفيفها. حيث على الرغم من أن تجنب المخاطر هو المسار الأكثر أمانا بشكل عام، إلا أنه في هذه الحالة، يعني ببساطة عدم استخدام "لينكد إن" أو وسائل التواصل الاجتماعي الأخرى. وهذه ليست دائما النتيجة المرغوبة للشركات التي تشجع موظفيها على استغلال تواجدهم على وسائل التواصل الاجتماعي للترويج للشركة وعملها.

وكما هو الحال مع أي تهديد، فإن الخطوة الأولى للحد من إمكانية التوظيف عبر "لينكد إن" هي ببساطة إدراك وجود هذا الاحتمال. يجب أن يساعد هذا الوعي المستخدمين على إدراك أن التقدير أمر مهم عند النظر في المعلومات التي ينشرونها على "لينكد إن" أو على أي منصة أخرى، لهذه المسألة. ويجب على المستخدمين التفكير في كيفية ظهور ما ينشرونه إلى ضباط المخابرات، وكيف يمكن استخدامه ضدهم.

كما أن القليل من ضبط النفس يمكن أن يقطع شوطا طويلا نحو الحد من اجتذاب الأشخاص كأهداف. حيث إذا كان شخص ما يعمل في مشروع حساس أو تقنية يحتمل أن تهم ممثلا معاديا، فإن الحكمة تملي الامتناع عن نشر هذه المعلومات في منتدى عام. فنشر تفاصيل المشاريع الحساسة ليراها العالم بأسره أمر غير حكيم، نظرا لخطر لفت انتباه ضباط المخابرات لها.

أما الخطوة الثانية فهي تحث المستخدم على أن يظل متشككا في أي طلب صداقة يرسله له الغرباء. بل وتزداد نسبة الشك إذا كان الشخص الغريب لديه صورة ملف شخصي جذابة أو رومانسية. يُنصح أيضا بمراجعة ملفات تعريف الأصدقاء أو زملاء العمل الذين يطلبون الاتصال بعناية للتأكد من أنهم الأشخاص الحقيقيون وليسوا المحتالين.

وإذا كان الشخص الذي يقبله المستخدم كاتصال يبدأ في إرسال الرسائل إليه بطريقة تبدو ثرثارة للغاية، أو تتضمن الكثير من الإطراء لشخصيته، يجب أن تزداد شكوكه أكثر. يجب أن يراقب بعناية العلامات التي قد تشير إلى أن المتصل به يحاول بناء الثقة وتطوير علاقة معه كموظف محتمل.

يمكن أن تشمل العلامات الأخرى لمحاولة التوظيف المحتملة عروضا لكتابة ورقة أو للسفر مجانا لحضور مؤتمر. يجب أن يكون المستخدم متشككا بشأن عروض توظيف مقدمة له بشأن وظيفة لم يتقدم لها، وهو تكتيك يستخدمه كثيرا ضباط المخابرات والمجرمون العاديون على حد سواء.

ويؤكّد ستيورات أنه على مستخدمي "لينكد إن" أن يتذكروا أيضا أنه بدلا من محاولة التوظيف، قد يحاول ضابط المخابرات ببساطة خداع مستخدم لفتح

يمكن لمسؤولي المخابرات استخدام «لينكد إن» للحصول على قوائم الموظفين في شركة أو وكالة معينة في غضون ثوان

وحتى إذا كان المرفق من مصدر موثوق، على المستخدم أن يكون حذرا إذا لم يكن يتوقعه أو إذا لم يكن هناك شيء صحيح. قبل الفتح أو النقر، من الجيد أن يتصل صاحب الحساب بالمرسل لتأكيد إرساله. ويلفت ستيورات إلى أن المتسللين يتحكمون في حسابات "لينكد إن" المحمية بكلمات مرور ضعيفة، ويستخدمونها لإرسال هجمات تستهدف جهات اتصال ضحية القرصنة غير المشكوك فيها.

ويختم سكوت ستيورات نصائحه لمستخدمي "لينكد إن"، وغيره من المنصات الإلكترونية، لتفادي تجنيدهم كجواسيس، قائلا "إذا كنت تشك في أن شخصا ما يحاول تجنيدك، فأنصحك بتعليق كل الاتصالات ثم الإبلاغ عن النهج المشتبه به إلى جهة الاتصال الأمنية الخاصة بالشركات أو الحكومة. وعلى الرغم من أنك رصدت محاولة التوظيف، فقد لا تكون الهدف الوحيد، وزملاؤك في العمل قد لا يكونون أذكياء مثلك. وقد يؤدي الإبلاغ عن هذه المحاولات إلى جعل الآخرين في مؤسستك على دراية بالمخاطر المستمرة".