التجسس عبر لينكد إن: تجنّب تحويلك إلى جاسوس

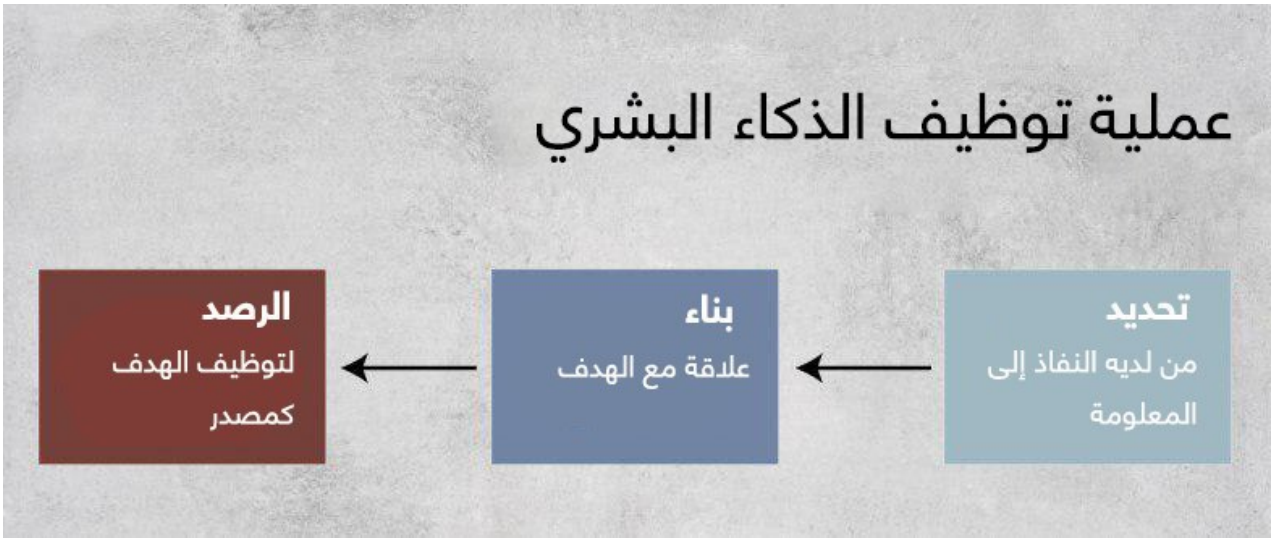
ترجمة وتحرير: نون بوست

أفادت تقارير انتشرت على نطاق واسع بأن هناك خطرا بشأن استخدام أجهزة الاستخبارات المعادية موقع لينكد إن كأداة توظيف، حيث ركز أحد هذه التقارير الذي أعده ميكا ألتولا من معهد السياسة الخارجية الفنلندي والصادر في حزيران/ يونيو 2019 على النشاط الصيني على لينكد إن. ولكن هذه الظاهرة لا تقتصر فقط على عمليات الاستخبارات الصينية ولا على هذه المنصة بالتحديد. في الواقع، تستخدم جميع وكالات الاستخبارات مآثر مماثلة، مثلما يتضح من الاختراق المرتبط بإيران لشركة ديلويت، الذي استُخدمت فيه إحدى الصلات على لينكد إن من أجل كسب ثقة أحد الموظفين.

مع ذلك، يشير عدد الحالات المُبلّغ عنها والمنسوبة إلى الصينيين، بما في ذلك تلك المتعلقة بضباط مخابرات سابقين على غرار كيفن مالوري وقضايا التجسس للشركات كتلك التي تورط فيها مهندس في جنرال إلكتريك للطيران، إلى أن أجهزة المخابرات الصينية تعد من بين أكثر المستخدمين نشاطا وعدوانية لموقع لينكد إن كأداة للتوظيف. ويجعل ذلك التخفيف من التهديد أمرا حاسما، سواء كان ذلك على لينكد إن أو أي منصة تواصل اجتماعي أخرى.

كيف تستخدم وكالات الاستخبارات العدائية موقع لينكد إن؟

تتطلب مواجهة التهديد الصادر عن لينكد إن فهمًا لكيفية استخدام أجهزة الاستخبارات له في عمليات التوظيف، وهو ما يمكن تحقيقه على أفضل وجه بالنظر إلى المنصة من خلال عدسة دورة توظيف الذكاء البشري. وتقوم عملية التوظيف على ثلاث مراحل أساسية، وهي التحديد والبناء والرصد. ويمكن تقسيم كل واحدة من هذه المراحل إلى خطوات أصغر. فضلا عن ذلك، قد يكون هناك قدر كبير من التباين في العملية وفقا للهدف والظروف. ولكن من أجل مقاصدنا، سيكون التركيز على هذه المراحل الثلاث كافيًا.



في مرحلة التحديد، يُعدّ ضباط الاستخبارات قائمة بالأشخاص الذين لديهم إمكانية الوصول إلى المعلومات المطلوبة ويرتبونهم وفقا لفرص الحصول عليها. والجدير بالذكر أنه قبل 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 هذه الخطوات الحصول على قائمة موظفي الشركة أو استخدام بعض الوسائل الأخرى للحصول على أسماء الأشخاص الذين يعملون على مشروع بعينه في شركة معينة. وفي بعض الحالات، قد يضطرون إلى توظيف عميل نفاذ داخل الشركة لتقديم المساعدة، وكل ذلك قد يستغرق بعض الوقت والجهد، وإذا لم يتم إنجازه بشكل ماهر، فقد يثير الشكوك في الشركة المستهدفة.

لكن في عالم وسائل التواصل الاجتماعي، يمكن لمسؤولي الاستخبارات استخدام موقع لينكد إن للحصول على قائمة الموظفين في شركة محددة أو وكالة معينة لها، فضلا عن مناصبهم فيها بالتحديد في غضون ثوان. وفي العديد من الحالات، يسرد الموظفون المشاريع أو التقنيات المحددة التي يعملون عليها، حتى أن بعضهم يقدم مستويات التصريح الأمني الخاصة بهم.

بمجرد تجميع ضابط الاستخبارات لقائمة الأهداف المحتملة، ستتمثل الخطوة التالية في تحديد أفضل الأشخاص المحتملين للتوظيف، والطريقة التي ستكون الأفضل للفوز بهم

على الرغم من أن أدوات وسائل التواصل الاجتماعي لا تعتبر طريقة مضمونة بالنسبة لضباط الاستخبارات من أجل إنشاء قائمة شاملة للجميع ممن لديهم إمكانية النفاذ إلى برنامج أو تقنية ما، إلا أنه يمكنهم بسهولة دفع عجلة هذه العملية. ومن خلال البحث عن زملاء العمل للأشخاص الذين وُضعوا في القائمة خلال عملية البحث الأولية، قد يتمكن ضباط الاستخبارات من إضافة أشخاص لم يكونوا منفتحين في ملفاتهم الشخصية على لينكد إن، إلى قائمة الأهداف المحتملة.

بمجرد تجميع ضابط الاستخبارات لقائمة الأهداف المحتملة، ستتمثل الخطوة التالية في تحديد أفضل الأشخاص المحتملين للتوظيف، والطريقة التي ستكون الأفضل للفوز بهم. وعند هذه النقطة أيضا، يمكن أن يكون لينكد إن مفيدا. وعلى الرغم من أن خدمة هذا الموقع موجهة للمحترفين، وهو في الواقع أكثر رسمية من منصات التواصل الاجتماعي الأخرى من قبيل فيسبوك وإنستغرام، إلا أن أعضاءها يشاركون عادة معلومات كافية لتقديم أدلة حول ماهية سير التوظيف.

على سبيل المثال، قد يكون أولئك الذين يجاملون باستمرار الأشخاص الجذابين مناسبين لمقاربة تنطوي على الإغواء. وبطريقة مماثلة، يمكن أن يكون أولئك الذين يشتكون من كونهم عاطلين عن العمل أو يعانون من العمالة الناقصة منفتحين أمام الإغراءات المالية. أما من يبدون غير سعيدين في العمل فيمكن أن يكونوا أكثر انفتاحا لتوظيفهم بدافع الحقد، فيما قد يستجيب أولئك الذين يشاركون منشورات بحثا عن تأكيد أنفسهم بشكل جيد لمحاولات تغذية غرورهم.

بالنسبة لموقع لينكد إن، فقد لاحظنا عدة حالات تقوم فيها وكالات الاستخبارات العدائية مثل الصين بتطوير علاقتها مع الشخص المطلوب من خلال تعريف نفسها على الموقع كمركز أبحاث أو جامعة

تُسهّل هذه المعلومات الوصول إلى الأهداف المحتملة وإقامة اتصال معها، وأشيرُ إلى الأهداف هنا، لأن إجراء هذه العمليات إلكترونيا يسمح حتى لضابط واحد بإقامة اتصالات مع أهداف متعددة قبل التركيز باهتمام أكبر على القلة التي تبدو واعدة وأكثر تقبلا، وبالتالي، زيادة احتمالات النجاح. ويمكن أن تتطور مرحلة التطوير في عملية التوظيف بشكل مختلف وفقا للهدف النهائي. وسيُطوّر نوع من عمليات التصيّد كتلك التي استخدمت في قضية شركة ديلويت بشكل مختلف عن العملية التي تتضمن محاولة لقاء المصدر شخصيا وتوظيفه. ولكن في كلتا الحالتين، يتمثل الهدف النهائي لمرحلة التطوير في بناء علاقة وبلوغ درجة من الثقة حتى يصبح الوصول للهدف الاستخباراتي ممكنا.

أما بالنسبة لموقع لينكد إن، فقد لاحظنا عدة حالات تقوم فيها وكالات الاستخبارات العدائية مثل الصين بتطوير علاقتها مع الشخص المطلوب من خلال تعريف نفسها على الموقع كمركز أبحاث أو جامعة. وبهذه الطريقة وخلف هذا الستار، تدفع هذه الوكالات الشخص لإعداد بحث حول موضوع ما، ثم تدعوه بعد ذلك في رحلة مدفوعة التكاليف إلى الصين لتقديمه (هذا في الواقع أحد الأشكال المعتمدة التي تُعرف باسم نهج "الخطاف الصغير"). بمجرد وصولهم إلى الصين، يتم تقييم الأشخاص الذين وقع اختيارهم بشكل أفضل، كما يتم تطوير العلاقة معهم بشكل أكبر وذلك لإتمام عملية التوظيف النهائية.

هناك طريقتان أساسيتان يمكن أن تساعد في التعامل مع التهديد أولهما محاولة تجنب المخاطر والتخفيف من حدتها

في بعض الحالات، وعند الضرورة قد تلجأ وكالة الاستخبارات إلى الاستعانة ببعض المستندات مثل مقاطع فيديو لمعاملات سابقة بين ضابط الاستخبارات والشخص المستهدف كشكل من أشكال الإكراه. وبمجرد تعيين الشخص المستهدف بشكل رسمي، يمكن ممارسة الضغط عليه لتقديم معلومات حساسة أكثر. وعلى الرغم من أنني ذكرت الصين على وجه التحديد، إلا أن جميع وكالات الاستخبارات تعتمد نفس النهج التي تعتمده الجهات الفاعلة في مجال المخابرات.

التعامل مع التهديدات

هناك طريقتان أساسيتان يمكن أن تساعد في التعامل مع التهديد أولهما محاولة تجنب المخاطر والتخفيف من حدتها. وفي حين يعد تجنب المخاطر من أكثر الطرق أمانًا، إلا أن ذلك يعني ببساطة عدم استخدام لينكد إن أو منصات التواصل الاجتماعي الأخرى، وهذا ما لا ترغب فيه الشركات التي تشجع موظفيها على استخدام وسائل التواصل الاجتماعي للترويج للشركة وعملها.

كما هو الحال مع أي تهديد آخر، فإن الخطوة الأولى التي يجب اتباعها للحد من عمليات التوظيف عبر منصة لينكد هي ببساطة إدراك وجود هذا الاحتمال. يجب أن يساعد الوعي بهذه التهديدات المستخدمين على إدراك أن التكتم مهم جدا لاسيما إذا تعلق الأمر بالمعلومات الشخصية التي ينشرونها على موقع لينكد إن أو أي منصة أخرى. لذلك، ينبغي على المستخدمين الأخذ بعين الاعتبار المعلومات التي يقدمونها إلى ضابط مخابرات عدائي، وكيف يمكن استخدامها ضدهم.

إذا كان الشخص الذي قبلته حديثا يتحدث بكثرة أو يجاملك دائما أو يبدو كما لو أنه يعمل على تضخيم صورتك، فعندها يجب أن تزداد شكوكك أكثر حوله

في الحقيقة، إن القليل من ضبط النفس يمكن أن يساهم في الحد من جاذبية المرء كهدف. إذا كان شخص ما يعمل على مشروع حساس أو تقنية يحتمل أن تهم ممثلا معاديًا، فإن الحكمة تملي الامتناع عن نشر هذه المعلومات في منتدى عام. إن نشر تفاصيل المشاريع الحساسة ليراها العالم بأسره أمر غير حكيم، نظرًا لأن ذلك يزيد من احتمال لفت انتباه ضباط المخابرات الخصوم. بناء على ذلك، يجب على مستخدمي لينكد إن النظر في كيفية ظهور ما ينشرونه لضباط المخابرات وكيف يمكنهم استخدام ذلك ضدهم.

بالنسبة للنقطة الثانية فهي متعلقة بالبقاء حذرا ومتشككا من كل الغرباء الذين يريدون التواصل معك من خلال لينكد إن. وعليك أن تشك أكثر في الأشخاص الذين يريدون التواصل معك وتكون صور حسابهم جذابة أو يقدمون مبادرات رومانسية. ويُنصح أيضًا بمراجعة ملفات تعريف الأصدقاء أو زملاء العمل الذين يطلبون التواصل معك بعناية للتأكد من أنهم الأشخاص الحقيقيون وليسوا محتالين.

إذا كان الشخص الذي قبلته حديثا يتحدث بكثرة أو يجاملك دائما أو يبدو كما لو أنه يعمل على تضخيم صورتك، فعندها يجب أن تزداد شكوكك أكثر حوله. يجب أن تراقب بعناية العلامات التي قد تشير إلى أن الشخص الذي تتواصل معه يحاول بناء الثقة وتطوير علاقة معك كموظف محتمل.

يمكن أن تشمل العلامات الأخرى لمحاولة التوظيف المحتملة عروضًا لكتابة ورقة أو للسفر مجانًا لحضور مؤتمر. لذلك عليك الشك في كل عرض يقدم لك من قبل متعهدي التوظيف المفترضين الذين يتعاملون معك حول وظيفة لم تتقدم لها من الأساس، وهو تكتيك يستخدمه كثيرًا ضباط المخابرات والمجرمون العاديون على حد سواء.

إذا كنت تشك في أن شخصًا ما يحاول تجنيدك، فإنني أنصحك بتعليق كل الاتصالات مع ذلك الشخص وتجنب المخاطرة، ثم الإبلاغ عن المشتبه به إلى جهة الاتصال الأمنية الخاصة بالشركات أو الحكومة

من جانب آخر، يجب أن يتذكر مستخدمو لينكد إن أنه بدلاً من محاولة التوظيف، قد يحاول ضابط المخابرات ببساطة خداع المستخدم لفتح البرامج الضارة. ونظرًا لتهديد التصيد العشوائي، يجب على المستخدمين توخي الحذر الشديد عندما يرسل الأشخاص الذين لا يعرفونهم جيدًا مرفقات أو روابط للبريد الإلكتروني. وحتى إذا كان المرفق من مصدر موثوق، فكن حذرًا إذا لم تكن تتوقعه أو إذا لم يكن هناك شيء صحيح.

قبل فتح الرابط أو النقر عليه، يجب عليك الاتصال بالمرسل لتتأكد من أنه هو من أرسل الرسالة. لسوء الحظ، بالطبع، من المعروف أن المتسللين يتحكمون في حسابات لينكد إن المحمية بكلمات مرور ضعيفة، واستخدامها لشن هجمات تستهدف جهات اتصال ضحايا القرصنة الموثوقين.

إذا كنت تشك في أن شخصًا ما يحاول تجنيدك، فإنني أنصحك بتعليق كل الاتصالات مع ذلك الشخص وتجنب المخاطرة، ثم الإبلاغ عن المشتبه به إلى جهة الاتصال الأمنية الخاصة بالشركات أو الحكومة.
وعلى الرغم من أنك رصدت محاولة التوظيف، فقد لا تكون أنت الهدف الوحيد وزملاؤك في العمل قد لا يكونون أذكياء مثلك.

المصدر: ستراتفور